Physician Date Banks: The Public's Right to Know Versus the Physician's Right to Privacy

Julie Barker Pape
PHYSICIAN DATA BANKS: THE PUBLIC'S RIGHT TO KNOW VERSUS THE PHYSICIAN'S RIGHT TO PRIVACY

Julie Barker Pape*

INTRODUCTION

In the 1980s, as the health care debate intensified and the number of medical malpractice suits rose dramatically, questions arose how best to improve the overall quality of health care.1 Because medicine is largely a self-regulating profession, one of the best ways to improve the quality of medical care practiced is to strengthen medical peer review,2 the process by which physicians monitor one another's treatment of patients to determine if staff privileges should be granted or denied, continued or terminated.3 Unfortunately, in the 1980s, peer review had been greatly stifled by the large treble damages awarded in the peer review antitrust lawsuits that became prevalent during that

---

* The author would like to thank Professors Joel Reidenberg and Benjamin Zipursky for their helpful information and comments on this Note.

1. See Health Care Quality Improvement Act of 1986, 42 U.S.C. § 11101(1) (1994) [hereinafter “HCQIA”] (“The increasing occurrence of medical malpractice and the need to improve the quality of medical care have become nationwide problems that warrant greater efforts than those that can be undertaken by any individual State.”).

2. When former Senator Albert Gore (D-Tenn.) introduced the HCQIA, he remarked, “In the long run, doctors themselves are in the best position to put an end to malpractice . . . .” Barbara A. Blackmond, Current Issues—The National Practitioner Data Bank and Hospital Peer Review, 7 Health Law, 1, 3 (1993), available in WESTLAW; see also HCQIA, 42 U.S.C. § 11101(3) (“This nationwide problem can be remedied through effective professional peer review.”).

3. “Peer review is the evaluation and monitoring of the qualifications and skills of physicians by their colleagues with whom they practice in a particular health care facility. The purpose of peer review is to monitor the quality, appropriateness and necessity of the medical care given to patients.” Jeanne Darricades, Comment, Medical Peer Review: How is it Protected by the Health Care Quality Improvement Act of 1986?, 18 J. Contemp. L. 263, 270 (1992). Peer review is usually conducted when a physician applies for staff privileges at a new hospital or when a physician’s conduct comes into question. The HCQIA calls peer review “professional review activity” and defines it as an “activity of a health care entity with respect to an individual physician—(A) to determine whether the physician may have clinical privileges with respect to, or membership in, the entity, (B) to determine the scope or conditions of such privileges or membership, or (C) to change or modify such privileges or membership.” 42 U.S.C. § 11151(10). Because almost every physician seeks staff privileges at some point in his career, peer review affects the vast majority of physicians.
This thinking lead to Congressional efforts to revitalize peer review.5

In an effort to bolster peer review and, consequently, the overall quality of health care, Oregon Congressional Representative Ron Wyden (D-Or.) introduced the Health Care Quality Improvement Act of 1986 (the “HCQIA”) on March 12, 1986.6 Based on the assumption that fear of huge antitrust lawsuits was preventing physicians from adequately reporting and disciplining their negligent colleagues, the HCQIA provides qualified antitrust immunity to peer review boards that follow certain procedures and guidelines.7 To obtain immunity, a peer review activity must be undertaken

(1) in the reasonable belief that the action was in the furtherance of quality health care, (2) after a reasonable effort to obtain the facts of the matter, (3) after adequate notice and hearing procedures are afforded to the physician involved or after such other procedures as are fair to the physician under the circumstances, and (4) in the reasonable belief that the action was warranted by the facts known after such reasonable effort to obtain facts and after meeting the requirement of paragraph (3).8

When peer review boards comply with these guidelines, they are immune from federal antitrust lawsuits.9

---

4. In the 1980s, many physicians who were denied staff privileges retaliated by filing lawsuits under the Sherman Antitrust Act, 15 U.S.C. §§ 1, 2 (1994), which allows a plaintiff whose right to conduct business has been compromised to collect treble damages. Exemplary of these suits is Patrick v. Burget, 486 U.S. 94, 99 (1988), in which the Supreme Court upheld a two million dollar treble damages award to a physician who sued for wrongful dismissal by a peer review board. In enacting the HCQIA, Congress recognized the harmful effect of cases like Patrick on peer review. See HCQIA, 42 U.S.C. § 11101(4) (“The threat of private money damage liability under Federal laws, including treble damage liability under Federal antitrust law, unreasonably discourages physicians from participating in effective professional peer review.”); see also Herbert G. Gleitz, et al., Practical Implications of the Health Care Quality Improvement Act 13-17 (Roxane C. Busey and Arthur N. Lerner eds., 1994) (discussing the effect of Patrick on the passage of the HCQIA).

5. See HCQIA, 42 U.S.C. § 11101(5) (“There is an overriding national need to provide incentive and protection for physicians engaging in effective professional peer review.”). See generally Blackmond, supra note 2, at 2-3 (discussing the seminal physician antitrust case, Patrick v. Burget, 486 U.S. 94 (1988), and the stifling effect it had on hospital peer review); Darricades, supra note 3, at 271-72 (discussing physician disincentives for participating in peer review).


7. The HCQIA requires that the peer review process incorporates due process and that peer review be undertaken only with the purpose of improving the quality of medicine practiced. 42 U.S.C. § 11112(a); see also Ilene D. Johnson, Reports to the National Practitioner Data Bank, 265 JAMA 407, 407 (1991) (discussing the immunity requirements of the HCQIA).


9. Id.
To aid physicians in peer review activities, the HCQIA mandated the establishment of the National Practitioner Data Bank to collect and disseminate to specified professional review entities disciplinary and malpractice information. The National Practitioner Data Bank contains information on malpractice judgments and settlement payments, disciplinary sanctions, and license suspensions and revocations. It was established to improve peer review by serving as an information clearinghouse that peer review boards and other medical authorities could check when evaluating a physician's ability to practice quality medicine. Indeed, the HCQIA requires peer review boards to check the National Practitioner Data Bank when making credentialing decisions and every two years thereafter. To improve physicians' confidence in the peer review process, the HCQIA provides limited antitrust immunity to those who check the National Practitioner Data Bank as required.

Information in the National Practitioner Data Bank is confidential and can only be disclosed to the entities specifically enumerated in the Data Bank regulations, primarily professional review authorities; the general public currently does not have access to any of the information in the National Practitioner Data Bank. The Office of the Inspector General of the Department of Health and Human Services can impose civil monetary sanctions on parties violating these confidentiality provisions.

Although the initial purpose of the National Practitioner Data Bank was to provide physician information to peer review boards, consumer

12. Id. § 11133.
13. Id. § 11132.
14. See id. § 11135.
15. Id. § 11135(a).
16. Id. § 11111(a). The HCQIA also grants immunity to those who provide information to peer review boards or the National Practitioner Data Bank. Id. § 11111(a)(2).
17. Those authorities include: a hospital requesting information concerning a medical practitioner on its staff or with privileges at the hospital; Boards of Medical Examiners or state licensing boards; health care entities who may be entering into an employment relationship or granting staff privileges to a health care practitioner; an attorney who has filed a suit against the hospital based on the hospital's failure to check the data bank regarding a specific practitioner; a health care entity with respect to peer review; and a physician accessing his own record. 45 C.F.R. § 60.11(a); see National Practitioner Data Bank for Adverse Information on Physicians and Other Health Care Practitioners, 45 C.F.R. § 60 (1996); see also National Practitioner Data Bank: Fact Sheet for the General Public (visited July 3, 1997) <http://www.npdb.com/factsheet/fsgenpub.htm> [hereinafter “NPDB Fact Sheet”] (providing general information about the National Practitioner Data Bank).
19. Id. § 11137(b)(2).
rights activists soon came to view the National Practitioner Data Bank as a valuable resource for evaluating physicians. Public activists, anxious about what they see as the declining quality of health care, believe that medical consumers should be able to use the National Practitioner Data Bank to screen their doctors and, thereby, avoid negligent ones.

Despite numerous efforts by patient rights advocates, however, the National Practitioner Data Bank has remained inaccessible to the general public. Not surprisingly, other publicly accessible sources for this information have emerged. For example, in November 1996, the state of Massachusetts established its own data bank to provide its citizens with information about Massachusetts physicians. Other states are currently implementing or plan to implement similar data banks.

The availability of this information has sparked tremendous debate. Medical consumers and consumer rights groups praise the Massachusetts data bank and argue that even more information about physicians and their practice histories should be disclosed to the public. At the same time, physicians and physician groups, such as the Ameri-

---

20. See Sidney M. Wolfe, Congress Should Open the National Practitioner Data Bank to All, Pub. Health Rep., July 1, 1995, at 378 (arguing that medical consumers should have access to the National Practitioner Data Bank).


22. See supra Part I.A (discussing consumer rights advocates' and Congressional efforts to publicize the contents of the National Practitioner Data Bank).


25. See, e.g., Editorial, Our View: Massachusetts is Taking the Mystery out of Doctors' Backgrounds. Other States Should Follow., USA Today, Oct. 31, 1996, at 10A (praising the Massachusetts data bank and arguing that other states should emulate it); Editorial, Physician Profiles: Handled Properly, Information Will Aid Consumers, Telegram & Gazette (Worcester, Mass.), Aug. 29, 1996, at A14, available in 1996 WL 2401559 (discussing the benefits of the Massachusetts data bank); Editorial, Public Deserves Data on Doctors' Records, The Tennessean, Jan. 4, 1997, at 10A (arguing that Tennessee should follow Massachusetts and establish a similar physician data bank); Laurel Shackelford, Patients Need Good Information About Their Doctors, The Courier-Journal (Louisville, Ky.), Nov. 17, 1996, at 2D (praising the Massachusetts data bank and arguing that other states should emulate it).
can Medical Association (the "AMA"), call for the eradication of such data banks, arguing that the information contained in the data banks is misleading to medical consumers and violative of physician privacy rights. This Note acknowledges the public's right to access physician information and make informed risk calculations, yet also argues that the physician data banks compromise certain physician privacy interests and that, when physicians are forced to protect their privacy, they will be less likely to disclose any information at all—severely hindering peer review and resulting in a cumulative negative effect on the quality of health care.

This Note discusses the controversy surrounding physician information and how the necessary information can be disseminated to medical consumers without compromising physician privacy and, in turn, the overall quality of health care. Part I provides background information on the National Practitioner Data Bank and other state data banks containing physician practice information. Part II discusses the public policy debate surrounding whether the information contained in these data banks should be made available to the general public and, if so, in what form and amount. Part III analyzes the privacy issues involved in this controversy by chronicling the concept of privacy as it has evolved in American common and statutory law, identifying physicians' existing legal interest in this information and discussing the unique privacy issues that must be considered when the information at issue is contained in an electronic data bank format. Part III also introduces "fair information practices," standards that have been formulated to maintain an electronic data bank in compliance with the privacy considerations established earlier in Part III. Part III determines that, because of the public's strong interest in receiving information about their doctors, physicians' privacy interests are best protected not by a right to withhold information, but by a right to ensure that information about them is collected and disseminated legitimately and responsibly. Therefore, part IV provides an ideal model for a federal physician data bank that provides medical consumers the information they need to make informed choices about


28. Dolores Kong, A Doctor's Past: Does the Public Have a Right to Know?, The Boston Globe, Nov. 28 1994, at 25 (discussing how, if doctors do not support making the information public, they will resist supplying the necessary information).

29. See supra note 2 (discussing the importance of peer review in quality health care).
their health care, but does not unnecessarily compromise physician privacy interests. Part IV argues that providing limited access to the National Practitioner Data Bank in accordance with "fair information practices" would best accomplish these objectives. Part IV first discusses the differences in privacy protection between the various states and between the states and the federal government, and concludes that, because of federal privacy laws already in place, a federal data bank has greater potential for incorporating fair information practices. Part IV then analyzes the application of fair information practices to the National Practitioner Data Bank and indicates which information should be disseminated and with what limitations and restrictions so as to allow limited public access with only minimal infringement of physician privacy interests.

I. PHYSICIAN INFORMATION DATA BANKS AND THE CONTROVERSY SURROUNDING THEIR ACCESSIBILITY BY THE PUBLIC

This part provides an overview of the National Practitioner Data Bank, the Massachusetts physician data bank, and other state data banks. This part first examines the functions and operations of the National Practitioner Data Bank and discusses the decision to maintain the confidentiality of its files. This part then discusses the Massachusetts and other state data banks that have been or will be created to give consumers access to physician information withheld from them by the National Practitioner Data Bank.

A. The National Practitioner Data Bank

The National Practitioner Data Bank, which was established as part of the HCQIA, is maintained by the Department of Health and Human Services and serves as a repository of physician information. The regulations established for the National Practitioner Data Bank require reporting of the following situations: any payment made by any individual or entity on behalf of a physician for the purposes of settlement, partial settlement, or to satisfy a malpractice claim, and any adverse licensing or disciplinary actions taken against a physician. Entities that are required to report this information are hospitals and other health care entities, the Board of Medical

---

30. NPDB Fact Sheet, supra note 17; see also Peter A. Setness, What Do You Know About the NPDB?, Postgraduate Med., July 1996, at 15.
32. HCQIA, 42 U.S.C. § 11133(a) (1994). A health care entity must report to the state Board of Medical Examiners if it takes a professional review action that affects a physician's clinical privileges for more than thirty days, if a physician surrenders privileges while under investigation or in return for not instigating an investigation, or—if a professional society—when it undertakes a peer review investigation that adversely affects a physician's membership in that society. Id. § 11133(a). The state's Board of
Examiners, and individuals and entities—including insurance companies—making payments as a result of medical malpractice actions or claims. The report should include the physician's name, a description of the act or conduct at issue, and any other pertinent information, including the amount of any malpractice judgment or settlement.

Information reported to the National Practitioner Data Bank is maintained so that it can be queried by state medical boards and peer review boards in the licensing, discipline, and peer review processes. Information contained in the National Practitioner Data Bank is available to “[s]tate licensing boards, to hospitals, and to other health care entities . . . that have entered (or may be entering) into an employment or affiliation relationship with the physician or practitioner or to which the physician or practitioner has applied for clinical privileges or appointment to the medical staff.” Physicians may also access the Data Bank, but only to check their own file.

The rationale for the National Practitioner Data Bank is two-fold: to prevent negligent physicians from moving to a new state to escape a record of incompetence in the previous state, and to improve peer review by providing qualified antitrust immunity to hospitals and their peer review boards if they check the National Practitioner Data Bank every two years as required.

Medical Examiners reports this information to the Secretary of the Department of Health & Human Services. Id. § 11134(b).

33. HCQIA, 42 U.S.C. § 11132. Each state’s Board of Medical Examiners must report to the Secretary any action that “revokes or suspends (or otherwise restricts) a physician’s license or censures, reprimands, or places on probation a physician, for reasons relating to the physician’s professional competence or professional conduct, or to which a physician’s license is surrendered.” Id. § 11132(a).

34. HCQIA, 42 U.S.C. § 11131. If such an entity fails to report, it is subject to a fine of not more than $10,000. Id. § 11131(c).

35. Id. § 11131(b), 11132(a)(2), 11133(a)(3).

36. Johnson, supra note 7, at 407. “Persons and entities may obtain information from the Data Bank by submitting a request in such form and manner as the Secretary may prescribe.” National Practitioner Data Bank for Adverse Information on Physicians and Other Health Care Practitioners, 45 C.F.R. § 60.11(b) (1996). For each transaction a fee is determined based on the use of the electronic data processing equipment in obtaining the information, the amount of photocopying that is needed, postage cost, and any additional costs such as express mail. 45 C.F.R. § 60.12(b).


38. Id. § 11137(b)(1); 45 C.F.R. § 60.11(a)(2).

39. Johnson, supra note 7, at 407. While states compile this information about their own physicians, an individual state cannot also keep records of the other forty-nine states. Thus, one advantage of the National Practitioner Data Bank is its national scope. Id.; see HCQIA, 42 U.S.C. § 11101(2) (“There is a national need to restrict the ability of incompetent physicians to move from State to State without disclosure or discovery of the physician’s previous damaging or incompetent performance.”).

40. HCQIA, 42 U.S.C. § 11135(a); see Setness, supra note 30, at 16. Hospitals and their peer review boards are assumed to have checked the National Practitioner Data Bank and to make decisions with knowledge of its contents. HCQIA, 42 U.S.C.
Since the National Practitioner Data Bank’s inception, however, there has been great controversy over the extent to which, if at all, it should be accessible to the general public.\textsuperscript{41} Congress debated the issue when the regulations for the Data Bank were promulgated, but decided that the information contained in the National Practitioner Data Bank would be confidential and inaccessible by the general public.\textsuperscript{42} If information is illegally obtained or disclosed, a penalty of not more than $10,000 may be imposed.\textsuperscript{43}

In April 1994, Representatives Ron Wyden (D-Or.) and Scott Klug (R-Wis.) introduced a bill into Congress, “The Health Care Quality Amendments of 1994,”\textsuperscript{44} which proposed that certain information in the National Practitioner Data Bank, including adverse malpractice actions and settlement payments made by practitioners with two or more incidents, be compiled in free, semiannual booklets available in public libraries.\textsuperscript{45} In addition, the proposed bill would have required that medical boards report license denials in addition to license suspensions and revocations, expanded National Practitioner Data Bank access to other provider networks, and required public hospitals and agencies, which previously did so only voluntarily, to report all adverse malpractice investigations.\textsuperscript{46} After this legislation failed, Representatives Wyden and Klug filed additional, unsuccessful legislation in 1995 attempting once again to open the Data Bank.\textsuperscript{47} Also in 1995, Senator Paul Wellstone (D-Minn.) proposed an amendment that would have opened the National Practitioner Data Bank to the public to the Senate Labor & Human Resources Committee, but the Committee rejected that proposal as well.\textsuperscript{48} In July 1996, another ulti-
mately unsuccessful bill was filed in the Senate that would have allowed public access to the records of the 6500 medical practitioners with at least three separate disciplinary actions or malpractice payments.\footnote{49. Your Health: Checking up on Your Doctor: What Can You Find Out?, Consumer Rep., Nov. 1996, at 62, 63 [hereinafter Checking up on Your Doctor].}

Although legislators’ efforts to provide public access to the information in the National Practitioner Data Bank have been unsuccessful thus far, much of the same information is nonetheless available elsewhere. In the private sector, various consumer and patients’ rights agencies have compiled and published information about physicians.\footnote{50. Id. at 62.}

For example, the Public Citizen Health Research Group, in addition to lobbying extensively to open up the National Practitioner Data Bank, has published its own compilation of negligent physicians, \textit{13,012 Questionable Doctors}.\footnote{51. See id.} Moreover, a California company has licensed the American Medical Association’s data bank of physician information and supplemented it with state and federal agency physician disciplinary records to provide consumers with reports about their doctors.\footnote{52. Id.}

\section*{B. The Massachusetts and Other State Physician Data Banks}

Concerned with the rising costs of health care and the public’s need to identify and avoid negligent doctors, many states are considering the creation of their own physician data banks to provide their citizens with information similar to that contained in the National Practitioner Data Bank.\footnote{53. See Gary F. Krieger, Should Your Patients Be Able to Learn All About You? (Public Disclosure of Information About Physicians), Am. Med. News, May 12, 1997, at 19 (“Massachusetts already has a program to do this. So does Maryland. Florida is about to start one, and most state legislators have bills designed in one way or another to increase public knowledge about doctors.”); see also Tait Trussell, No System Perfect in Trying to Protect Health of Patients, Orlando Sentinel, Dec. 8, 1996, at 3, available in 1996 WL 12432089 (discussing Florida’s contemplation of a physician data bank).}

Massachusetts became the first state to enact such a law\footnote{54. Massachusetts Act, supra note 23; see also Donohue, supra note 23 (discussing the effects of the Massachusetts Act and including the Act in Appendix I).} when it opened the nation’s first toll-free consumer hotline through which medical consumers can access information about their physician’s practice history.\footnote{55. See Editorial, Disclosing Doctors’ Records Can Only Help Patients, USA Today, Oct. 31, 1996, at 10A; Bruce Mohl, Now Consumers Can Give Their Doctors a Checkup, Boston Globe, Nov. 7, 1996, at A1. The Massachusetts data bank can be reached by telephone at (800) 377-0550 and (617) 727-0773, Bruce Mohl, State Deluged by Requests for Doctor Records, Boston Globe, Nov. 14, 1996, at A36, by mail at Board of Registration in Medicine, Attn: Profiles, 10 West St., Boston, MA 02111. \textit{id.}, or through the Internet. \textit{See infra} note 62 and accompanying text.} Before implementing its data bank, the Massachusetts Secretary of Consumer Affairs appointed an Advisory
Committee on Public Disclosure of Physician Information (the "Advisory Committee") to determine what information should be disclosed and the most effective means of disseminating it.\textsuperscript{56} The Advisory Committee decided that "[a]ll reliable information in the [State Medical] Board's possession that could be helpful to the public in choosing doctors should be released, unless there is a compelling public policy reason for keeping it confidential."\textsuperscript{57} The information currently available through the Massachusetts hotline includes malpractice payments (including settlements), disciplinary actions, criminal charges, education and awards, hospital affiliations, and insurance plans and specialties.\textsuperscript{58}

The Massachusetts data bank, maintained and operated by the state's Board of Registry in Medicine, currently contains 27,000 physician report cards\textsuperscript{59} and has been used extensively in its first few months of existence.\textsuperscript{60} Based in part on the perceived success of the Massachusetts data bank, other states, including Florida, Maryland, and New York, are considering similar physician information data bank programs.\textsuperscript{61} In addition, whatever potential benefits and detriments that will result from frequent access of the Massachusetts data bank will be amplified now that the Massachusetts data bank is accessible through the Internet.\textsuperscript{62}


\textsuperscript{57} \textit{Id.} at 128 (quoting the Massachusetts Advisory Committee on Public Disclosure of Physician Information) (emphasis omitted).

\textsuperscript{58} Online, the categories are (1) demographics of each doctor's practice; (2) education and training; (3) awards received and participation in peer review publications; (4) disciplinary history; and (5) paid malpractice claims. Massachusetts Physician Profiles, (visited Sept. 11, 1997), \texttt{<http://www.docboard.org/ma/ma_home.htm>}; \textit{see also} Donahue, \textit{supra} note 23, at 115 (discussing the Massachusetts data bank); David Armstrong, \textit{Background Profiles on Mass. Physicians Available on Internet}, Boston Globe, May 1, 1997, at B2 (same); Editorial, \textit{Disclosing Doctors' Records Can Only Help Patients}, USA Today, Oct. 31, 1996, at 10A (same).


\textsuperscript{60} On the first day the Massachusetts hotline was open, it received more than 500 calls by early afternoon. Associated Press, \textit{Phone Lines Busy in Mass. as Public is Given Access to Doctors' Profiles}, Lexington Herald Leader, Nov. 8, 1996, at A7. Between November and May, the Massachusetts data bank received more than 50,000 requests. Armstrong, \textit{supra} note 58, at B2.

\textsuperscript{61} See Krieger, \textit{supra} note 53, at 19.

electronic medium is a boon to patient rights advocates, it raises concern for physician privacy rights to new levels.63

II. Policy Arguments Surrounding Public Access to Physician Data Banks

Although the goal for both sides in this debate is an overall improvement in health care, the question is how best to achieve it. Patient rights advocates favor providing consumers with more information about their doctors,64 while the medical profession maintains that the confidentiality necessary for effective peer review should be preserved.65 This part examines this policy debate. First, it discusses the two main arguments advanced in favor of providing medical consumers with access to physician information: (a) informed consent and (b) protection against future medical malpractice. Second, it analyzes the medical profession's fears that weakening the confidentiality of physician data banks will have a deleterious effect on the quality of health care because physicians will compensate by spending more time protecting their reputations and defending frivolous claims and less time monitoring their negligent colleagues and practicing quality medicine.

A. Arguments in Favor of Widespread Dissemination of Physician Information

Patient rights advocates note that "Americans today have more performance information available to them when purchasing breakfast cereal than when choosing a heart surgeon."66 This statement is a call to arms for patient rights advocates across the country in their fight to make information about physicians' practice history available to medical consumers.67 As medical malpractice incidents increase and costs of health insurance climb higher, patient rights advocates feel it is becoming increasingly important to empower citizens to make informed choices about the quality of health care they receive. To make such informed choices, they argue, it is imperative that medical consumers receive information about the physicians in whose hands they entrust the health and well-being of themselves and their families.68

63. See infra Part III.B.1 (discussing the particular problems and unique privacy issues implicated in publishing controversial information in a widely-available electronic format).
64. See infra Part II.A.
65. See infra Part II.B.
66. This statement was communicated by Rep. Ron Wyden (D-Or.) in his fight to provide medical consumers with increased access to information about their physicians. See Wyden, supra note 40, at 380.
68. See supra notes 20-21 and accompanying text.
1. Informed Consent

The strongest argument for giving medical consumers information about their physicians is based on the doctrine of informed consent, which holds that to avoid committing a battery or negligence a physician must fully inform a patient of all risks associated with a procedure. If the patient is fully informed and consents to the treatment, such consent mitigates against a claim of negligence brought against the physician. At the same time, if a patient is not fully informed, the patient's consent is meaningless. Patient rights advocates argue that without the information contained in physician data banks, a patient is not fully informed. They seek to empower medical consumers by providing them with information about their physicians, arguing that such information is central to a patient's decision whether to see a certain physician. When this information is kept from patients, it detracts from the patient's decision-making power and reinforces the imbalance in power between the physician and patient. "Increased public access to information would be consistent with the policy of encouraging individual responsibility for behavior, as opposed to relying on paternalistic control by government." The strong protection that the informed consent doctrine affords patients is clearest at the state level. Several state cases reinforce the patient's right to know information about their physician that may affect the physician's ability to practice medicine—information that

69. For a general discussion of the tort doctrine of informed consent, see William L. Prosser et al., Cases and Materials on Torts 90-102 (9th ed. 1994).
70. James E. Ludlam, Informed Consent: Legal Theory and Clinical Practice 8-11 (1978) (discussing what a patient should be told to satisfy "informed consent").
71. Consent is generally considered a defense to a tort. See, e.g., Prosser, supra note 69, at 90-102. See generally Ludlam, supra note 70, at 11-14 (describing the extent of the physician's duty).
72. Douglas P. Biklen et al., American Association on Mental Deficiency, Consent Handbook 8 (H. Rutherford Turnbull III ed., 1977) ("Consent is ineffective unless a person has information about the matter (e.g., medical treatment) for which consent is sought.").
74. Id. ("Theoretically, a duty to disclose would maximize the autonomy of both providers and patients. . . . Patients who received appropriate information could choose whether to encounter the risks presented by a particular provider. . . . Patients would not be forced to encounter risks that, given knowledge, they would choose to avoid.").
75. Miller, supra note 56, at 125.
76. Elisabeth Ryzen, The National Practitioner Data Bank: Problems and Proposed Reforms, 13 J. Legal Med. 409, 457 (1992). Such empowerment is further augmented by maintaining the information in an easily accessible electronic format. See Robert S. Peck, Extending the Constitutional Right to Privacy in the New Technological Age, 12 Hofstra L. Rev. 893, 897 (1984) ("[T]he accessibility to data processing capabilities made possible by powerful personal computers has a decentralizing impact, taking information power away from government and large business organizations and giving it to a newly computer-literate populace.").
would influence the patient's decision whether to see that physician. For example, the Louisiana Court of Appeals in *Hidding v. Williams* held that a surgeon's failure to inform his patient of his chronic alcohol abuse constituted a breach of informed consent. The court held that “[b]ecause this condition creates a material risk associated with the surgeon’s ability to perform, which if disclosed would have obliged the patient to have elected another course of treatment, the fact-finder’s conclusion that non-disclosure is a violation of the informed consent doctrine is entirely correct.” Other states have relied on similar logic to identify information, such as a physician’s economic incentives for performing certain treatments or the physician’s HIV status, that would influence a patient’s treatment decision and therefore must be disclosed to avoid an informed consent violation.

This theory fails to provide adequate justification for releasing all physician information in a form accessible to anyone. The doctrine of informed consent is based on the duty that arises from the physician-patient relationship. The physician-patient relationship is not established until treatment begins. Thus, where there is no specific doctor/patient relationship—only a relationship between a physician and the public at large—the informed consent doctrine is inapplicable.

2. Protection Against Future Medical Malpractice

A second argument in favor of disclosure of the information in physician data banks is that it will decrease future medical malpractice by allowing medical consumers to identify and thereby avoid incompetent practitioners. Consumer rights advocates have compiled a
plethora of grisly patient horror stories in which patients suffer grievous malpractice injuries only to later learn that the negligent physician had a history of incompetence which, because this information was not widely available, the patient had no way of efficiently discovering. Patient rights advocates' desire to limit or eliminate the practice of negligent physicians is consistent with the Congressional rationale for establishing the National Practitioner Data Bank. Congressional supporters of the HCQIA worried that, without a central monitoring mechanism like the National Practitioner Data Bank, negligent physicians would be able to commit malpractice in one state, even receive appropriate discipline, but then move to another state and practice unfettered. Practicing in a new locale, they could conceivably commit future malpractice because there was no convenient way for the latter state to discover the physician's history in the former state. According to Sydney Wolfe, Director of the Public Citizen Research Group, an organization that has published its own list of allegedly negligent doctors, "[A]s long as the information in the Data Bank is kept from the public, most malpracticing physicians will escape punishment for their behavior."

continue to practice medicine. Della De Lafuente, Consumer Critique: AMA Scoffs at "Dubious Doctors" List, Chicago Sun-Times, March 29, 1996, at 39, available in 1996 WL 6738281. Consumer rights advocates argue that medical consumers have a right to be informed and avoid these negligent practitioners. Wyden, supra note 40, at 380 ("[C]onsumers have a right to know more about which health care providers they may wish to avoid... The last thing consumers need is for the Federal Government to withhold vital quality information from them.").

85. See Margolis, supra note 41, at 24 (providing the example of a parent who learned only after her daughter's death that the responsible party, her child's neurosurgeon, had a record of malpractice in numerous states, yet continued to hold licenses in seven states); Laurel Shackelford, Patients Need Good Information About Their Doctors, The Courier-Journal (Louisville, Ky.), Nov. 17, 1996, at 2D (describing how a family learned only after a Colorado anesthesiologist caused the death of their eight-year-old child by allegedly falling asleep during the child's ear surgery that the doctor had a history of falling asleep during surgery).

86. The HCQIA established the National Practitioner Data Bank to provide a central mechanism for identifying negligent practitioners. HCQIA, 42 U.S.C. § 11101(2). The HCQIA, however, placed the responsibility for ensuring that negligent physicians cease harmful practices solely on the medical profession itself, through its peer review boards, and not on potential patients. See id. §§ 11132, 11133; see also id. § 11137 (mandating the confidentiality of the Data Bank's contents).

87. HCQIA, 42 U.S.C. § 11101(2) (finding that incompetent physicians' ability to move from state to state necessitated a national remedy).

88. Johnson, supra note 7, at 407; Brian C. Mooney, The Patients Left Behind: Doctors with Dubious Records Start Fresh in Other States, The Boston Globe, Oct 5, 1994, at 1. The purpose of the National Practitioner Data Bank, however, was to prevent such occurrences by enlightening state licensing and local peer review boards, not by providing this information to the general public who may or may not have a legitimate use for it. See infra Part IV.B.4 (determining the physician information for which the public has a legitimate use).

89. Margolis, supra note 41, at 25 (quoting Sydney Wolfe). But see Part IV.B.4 (arguing that certain information contained in the National Practitioner Data Bank,
Because of both the long-standing tradition of protecting informed consent and the strong public policy in favor of improving the quality of health care, there has been great support in the courts, legislatures, and communities throughout the country for the proposition that information about a physician's practice history is a valuable commodity that should be accessible to the general public.\textsuperscript{90} Although there are physician privacy interests involved in the information at issue,\textsuperscript{91} consumer rights advocates and others argue that when these privacy interests are balanced against the compelling public need for this information,\textsuperscript{92} this public need outweighs physicians' privacy interests.\textsuperscript{93}

B. Policy Arguments Against Disclosure of Physician Information

Although medical consumers desire access to physician information to improve the quality of individual health care, providing increased access to physician information may actually have a deleterious effect on the overall quality of health care by (a) increasing litigation and detracting from physicians' medical responsibilities and (b) removing the confidentiality necessary for effective peer review and, consequently, decreasing the amount of self-policing practiced by the medical profession.

1. Increase in Medical Malpractice Litigation

While it may appear that access to physician information will aid consumers, it may actually harm them through the long-term effects disclosure could have on health care quality and costs. The medical profession argues that exposing physicians to such publicity threatens both their reputation and privacy.\textsuperscript{94} Physicians' efforts to reaffirm both will create an explosion in medical malpractice litigation as physicians seek to avoid being reported to these data banks.\textsuperscript{95} Where physicians were more willing to settle frivolous actions, they will now

\begin{itemize}
  \item such as malpractice settlement payments, is not necessarily an accurate predictor of future negligence).
  \item See generally Miller, \textit{supra} note 56 (arguing in favor of public access to physician information).
  \item See infra Part III (arguing that physicians have a valid, but limited, privacy interest in this information).
  \item See generally Bobinski, \textit{supra} note 73, at 294-309 (discussing the types of risks that a physician can present to an uniformed patient).
  \item But see infra Part III.C. (discussing the balancing test in regards to physician data banks and concluding that consumers' information needs are best met, not by total disclosure, but by partial disclosure in accordance with the demands of fair information practices to provide the public with information while simultaneously protecting physicians' privacy).
  \item Kong, \textit{supra} note 28, at 25 (reporting doctors', insurance officials', and state regulators' fears that malpractice information could be "unnecessarily damaging to a physician's reputation").
  \item Already, there is evidence that physicians have assumed a "fight to the death" mentality to avoid having a file in these data banks. Ryzen, \textit{supra} note 76, at 434.
\end{itemize}
be forced to defend them in order to avoid the data banks' negative consequences.\textsuperscript{96} An increase in medical malpractice litigation not only affects physicians and their insurance companies,\textsuperscript{97} but the general public as well—increased expenses resulting from additional litigation\textsuperscript{98} will be passed on to medical consumers through overall increases in health care costs.\textsuperscript{99} In addition, physicians spending more time and money litigating frivolous lawsuits are spending less time and energy practicing good medicine.\textsuperscript{100}

2. Decrease in Medical Peer Review

When physicians' privacy interests are threatened, it has a negative effect on peer review because it undermines physicians' trust in the peer review process and their willingness to share information about themselves and their colleagues.\textsuperscript{101} Although the HCQIA mandates the reporting of physician behavior by peer review and disciplinary boards,\textsuperscript{102} logically the National Practitioner Data Bank can only receive this information when the various local peer review and discipli-

\textsuperscript{96} According to Martin J. Hattlie, the American Medical Association's professional liability expert, "We already know the data bank has had the unintended effect of making physicians reluctant to settle lawsuits... So the verdict's still out on whether the data does more harm than good." Linda Oberman, \textit{IG Asks Why More Hospitals Don't Report Adverse Actions}, Am. Med. News, Feb. 13, 1995, at 4, available in 1994 WL 12763046 (quoting Martin J. Hattlie). In addition, the Physicians Insurers Association of America reported that, in 1993, ninety-seven percent of their companies reported that physicians were less willing to settle cases because of the National Practitioner Data Bank. James S. Todd, \textit{Just Numbers or Knowledge?}, Pub. Health Rep., July-Aug. 1995, at 377.

\textsuperscript{97} The California Large Loss Trend Study reported that "[p]roceeding to trial in 1991 cost an average of 66 percent more than in 1990." Ryzen, \textit{supra} note 76, at 435.

\textsuperscript{98} While giving the public access to physician data banks may have the immediate, undesired effect of increasing the costs of and time spent on litigation, it is possible that public access to the data banks may limit litigation costs in the long run if plaintiffs' attorneys who normally take cases on a contingency basis realize that they will be forced to fight frivolous claims to the end—with a risk of recovering nothing as compared to the previous instance of an assured settlement—and cease to represent such claims. This result, however, may also be harmful to the overall quality of health care. In the short run, physicians risk losing time and money spent litigating frivolous claims; while in the long run, we risk chilling legitimate claims by persons who cannot otherwise afford to litigate their claims on a non-contingency fee arrangement.


\textsuperscript{100} In addition to spending less time practicing medicine, physicians may refuse to treat the more difficult or risky cases to avoid such liabilities. Castrone, \textit{supra} note 21, at 3D.

\textsuperscript{101} See Gail N. Friend et al., \textit{The New Rules of Show and Tell: Identifying and Protecting the Peer Review and Medical Committee Privileges}, 49 Baylor L. Rev. 607 (1997) (discussing, in the context of Texas's current peer review privilege, the rationale for peer review confidentiality and arguing that, to preserve peer review, this privilege should be protected); see also Wood, \textit{supra} note 59, at 65 (noting how peer review is already compromised by physicians' tendency to protect one another). "Medicine has a good old boys' network like every other business." \textit{Id}. (quoting Jim Perdue, a Houston medical malpractice attorney).

\textsuperscript{102} HCQIA, 42 U.S.C. §§ 11132, 11133 (1994).
nary boards have it to give. For example, peer review decisions, which the peer review boards are required to report, can only be obtained if the peer review process is functioning effectively. Because an effectively-functioning peer review process is dependent on the accurate reporting of a physician's behavior by both the physician himself and his colleagues, it is essential that physicians be able to trust the process. When physicians have increased fear that such information will eventually find its way into the public sphere, they may be less likely to report even potential problems and thus curtail future negligence.

For this reason, many states have sought to protect the peer review process by granting confidentiality to its proceedings. States such as Kentucky and California, for example, have statutes that specifically make peer review reports and proceedings confidential and inadmissible for purposes of discovery or evidence. Such state statutes are based on the idea that confidentiality of peer review contents

103. Id. § 11133.
105. "[H]ospitals fear that doctors no longer will participate in any meaningful way on peer review committees—mandated by federal law—if the meetings are not kept confidential." Kathy Robertson, Court Lifts Lid on Peer Review, Bus. J. (Sacramento, Cal.), Oct. 14, 1996, at 1, available in 1996 WL 12821859 (reporting the medical community's fears and reactions to a California Supreme Court decision granting the California Medical Board access to peer review files); see also Kathy Robertson, Top Court Lifts Lid on Peer Reviews, San Antonio Bus. J., Oct. 21, 1996, available in 1996 WL 11762810 ("[D]octors won't be willing to participate on the voluntary panels if they know the information may be used by state agencies . . . .") (quoting Kim Davenport, legal counsel to the California Medical Association)).
106. Darricades, supra note 3, at 272-73. The privileges granted by states, however, do not extend to cases arising under federal law. Id.
109. "Currently, all fifty states have statutes giving varying degrees of protection to certain medical peer reviewers." Bloemer, supra note 107, at 276 (footnote omitted). Some of this protection is immunity from civil action similar to that granted by the HCQIA. Id.; HCQIA, 42 U.S.C. § 11112 (1994).
110. These statutes do not contradict the HCQIA's provisions. The HCQIA requires that peer review boards report adverse decisions affecting a physician's clinical privileges for more than thirty days, id. § 11133(a), not every peer review proceeding in which a physician may be involved. When the proceeding results in sanctions, the HCQIA gives discretion as to what evidence should be included in the National Practitioner Data Bank. Id. § 11133(a)(3). In addition, as the National Practitioner Data
is essential to encourage physicians' participation in the peer review process and to assure physicians that the identification of negligent colleagues improves the overall quality of health care practiced in their organization rather than just stigmatizes their colleagues.

Another reason for protecting the confidentiality of peer review proceedings is that the physician has only limited due process rights when investigated by a peer review board. Although the HCQIA places due process requirements on the peer review process, a peer review proceeding is not a trial and does not fully protect a physician's due process rights. For example, numerous courts have affirmed that a physician does not have a right to bring a private cause of action alleging due process infringement against a peer review board for actions taken against him. Therefore, a physician could witness the destruction of his professional reputation without adequate opportunity to defend himself or obtain reparation.

III. ANALYSIS OF THE PHYSICIAN PRIVACY INTEREST

This part discusses the existence of a physician privacy interest that must be weighed against the public policy favoring information dissemination. First, this part chronicles the concept of privacy as it has evolved in American constitutional and tort law and attempts to identify a physician privacy interest based on traditional constitutional and tort law principles found in judicial models for deciding when a privacy right has been breached and deserves redress. Second, this part discusses the new privacy considerations that accompany information contained in electronic data banks and online sources, and presents the use of "fair information practices" to best ensure the privacy of information collected in and disseminated from an electronic medium. Finally, this part argues that, while there is no explicit physician privacy interest redressible under tort or constitutional law, the principles of these traditional privacy frameworks should be extrapolated.
lated to create a proactive data privacy model using "fair information practices" to protect sensitive physician information before problems arise that necessitate physicians' recourse in the courts. Such a model would allow dissemination of physician information, but would also encourage the public's and physicians' participation to ensure that any dissemination is done responsibly and fairly. This Note ultimately concludes that, because medical consumers have a valid right to calculate their own risk in selecting physicians, the best way to accomplish this goal without also jeopardizing the quality of peer review and overall health care is to allow dissemination of physician information, but in a manner ensuring that physicians' privacy rights are not unnecessarily compromised.116

A. A Historical Basis for a Physician Privacy Interest

1. What Is Privacy?

A general privacy interest was first articulated by Louis D. Brandeis and Samuel D. Warren in their famous Harvard Law Review article, The Right to Privacy.117 Although their article was directed towards the actions of the press, it set the foundation for an individual's right to be protected from having his private affairs made public.118 Although the Warren and Brandeis article identified a potential right of privacy, there is no current all-encompassing definition of privacy. Despite numerous attempts over the past 100 years to define and delineate privacy, it has remained an elusive concept—it is difficult to pin down exactly what it entails and of what its boundaries comprise.119 For example, some scholars have interpreted privacy as a property right, seeing the information a person holds about himself as informational property that the individual alone controls and determines to whom it should be given.120 Another way of defining privacy

---

116. See infra Part IV (providing a model for a federal data bank that allows dissemination of physician information, yet includes standards to ensure that this dissemination is accomplished in the least privacy-threatening manner as possible).


119. See David H. Flaherty, On the Utility of Constitutional Rights to Privacy and Data Protection, 41 Case W. Res. L. Rev. 831, 831-35 (1991); see also Peck, supra note 76, at 899 (discussing the numerous ways of interpreting a right of privacy).

is to view it as an integral component of autonomy—the right of an individual to define his own personality, to make choices that determine who he is and how the outside world views him.\textsuperscript{121} The control of personal information is important for autonomy because the accumulation of information provides power.\textsuperscript{122} For this reason, privacy is better understood as a right to be protected than as a fault to be redressed.\textsuperscript{123} Under the autonomy formulation, maintaining privacy standards complies with the democratic notion of keeping power in the hands of the people and limiting government encroachment into the lives of citizens.\textsuperscript{124}

Privacy advocates who view privacy as a measure of autonomy tend to see it as a constitutional right meriting protection.\textsuperscript{125} The courts, however, have been extremely reluctant to find such a general, all-encompassing fundamental right to privacy.\textsuperscript{126} Instead, the traditional manner in which the courts have interpreted privacy has involved two distinct types of constitutional privacy rights—decisional rights, an individual’s right to make decisions about how he lives his life;\textsuperscript{127} and informational rights, an individual’s right to determine how others see him by controlling the information that the general public has about him.\textsuperscript{128} Because it gives a more concrete form to the information, which then becomes a commodity that can be bought and sold on the open market. Chlapowski, supra, at 158.

\textsuperscript{121} Chlapowski, supra note 120, at 150-55; Lawrence O. Gostin et al., Privacy and Security of Health Information in the Emerging Health Care System, 5 Health Matrix 1, 21-22 (1995) [hereinafter Gostin]; Peck, supra note 76, at 899.

\textsuperscript{122} Setting Standards, supra note 118, at 497 (“Because the control of information means power, standards for the treatment of personal information have significant societal implications.”).

\textsuperscript{123} Cf id. at 497-98; see Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, June 6, 1995, at 5 (visited Oct. 28, 1997) <http://www.itf.nist.gov/ipcipc-pub.html> (noting that a “critical characteristic of privacy is that once it is lost, it can rarely be restored”) [hereinafter Privacy Working Group Report]; see also infra Part IV (arguing for a proactive model to protect physician privacy before physicians need seek a judicial remedy).

\textsuperscript{124} In this manner, the right of privacy protects individuals’ “human dignity” by allowing them to create and maintain their own unique identity. Setting Standards, supra note 118, at 498.

\textsuperscript{125} Chlapowski, supra note 120, at 150. Chlapowski’s note argues that courts should recognize a fundamental right to informational privacy. “Informational privacy must be deemed an important, if not fundamental, right to receive any substantive treatment as an aspect of ‘liberty’ under existing due process norms.” Id. at 157; see also Flaherty, supra note 119, at 852 (arguing for a constitutional right to “privacy, data protection, and informational self-determination”); Paul M. Schwartz, The Protection of Privacy in Health Care Reform, 48 Vand. L. Rev. 295, 315 (1995) (“When the government collects personal data, a constitutional right to informational privacy applies.”).

\textsuperscript{126} Graham, supra note 118, at 1417 (discussing courts’ inability to fit claims into the existing privacy framework); see also Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law: A Study of United States Data Protection 76-89 (1996) (discussing American courts' traditional treatment of informational privacy).

\textsuperscript{127} Whalen v. Roe, 429 U.S. 589, 599-600 (1977) (defining a decisional right as “the interest in independence in making certain kinds of important decisions”).
Although the Constitution does not explicitly discuss privacy, the Supreme Court has interpreted the Constitution to imply a right to privacy that includes a number of decisional privacy rights. The Supreme Court has not, however, established a fundamental right to informational privacy. This Note argues that while physicians clearly lack a fundamental right to informational privacy, traditional privacy principles and case law nonetheless indicate that physicians have a privacy interest implicated by the collection and dissemination of information contained in physician data banks.

2. The Government’s Right to Collect Physician Information

Because physicians do not have an absolute right to informational privacy, the first part of the inquiry is to determine what interest they have in protecting against the collection of data in government data banks. The seminal case involving informational privacy and the government’s collection of information about its citizens is Whalen v. Roe.

Similar to the situation at issue in this Note, Whalen concerned private individuals’ rights against the Government’s ability to mandate the collection of information about them obtained from third parties. In Whalen, the Supreme Court decided whether a New York statute that required pharmacists and doctors to report prescriptions of certain drugs for compilation in a state data bank was viola-

128. United States Dep’t of Justice v. Reporters Comm. for the Freedom of the Press, 489 U.S. 749, 763 (1989) (defining an informational right as “the individual’s control of information concerning his or her person”); Whalen, 429 U.S. at 599 (defining an informational right as an “individual interest in avoiding the disclosure of personal matters”).

129. See, e.g., Roe v. Wade, 410 U.S. 113 (1973) (right to choose an abortion); Griswold v. Connecticut, 381 U.S. 479 (1965) (right to make decisions concerning contraception); see also Whalen, 429 U.S. at 597 n.18 (listing cases that involve decisional privacy rights); Paul M. Schwartz, Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 Iowa L. Rev. 553, 575-82 (1995) [hereinafter Privacy and Participation] (distinguishing between “independence in decisionmaking” and “avoiding disclosure of personal matters”). Although there is much debate concerning the bounds of decisional privacy, it is beyond the scope of this Note and is mentioned here only to illustrate the different treatment afforded informational privacy.

130. The court’s definition of an informational privacy right is important because a privacy right only merits full protection if it is found to be “fundamental,” or “implicit in the concept of ordered liberty.” Paul v. Davis, 424 U.S. 693, 713 (1976) (limiting fundamental rights to those dealing with “marriage, procreation, contraception, family relationships, and child rearing and education”).

131. This Note defines the prerogative that physicians have in protecting their privacy as a “privacy interest”—it is not an absolute or actual right; but rather, a privacy claim that must be weighed against and tempered by the considerations of the public. See infra Part III.C (balancing the public’s right to receive physician information against physicians’ rights to protect the privacy of such information and concluding that, in this context, a physician’s privacy interest is not in withholding information, but in ensuring its responsible collection and dissemination).


133. Id. at 591.
tion of privacy interests. The Supreme Court declined to find a fundamental right of informational privacy and employed only a rational relationship test. The Court looked at the actual information in the data bank to determine whether it was a rational solution to a legitimate problem—did it serve a legitimate state purpose?—and found that it did. Thus, after Whalen, it appears that federal and state governments can constitutionally collect information on the performance of their physicians. The Whalen analysis, however, does indicate that the government must have a legitimate purpose for doing so. While monitoring physicians is arguably a legitimate state purpose, the implication from Whalen is that the government’s ability to maintain physician data banks may be predicated on its agreement to collect and maintain information in a fair manner and only for legitimate purposes.

3. The Government’s Ability to Disseminate Physician Information

Once it is established that the government may collect the information, two related questions emerge: What is the government’s responsibility once it has accumulated this information and, is an individual’s right to privacy violated by the dissemination of information from this government data bank. Although Whalen found the government’s reasons for collecting personal information paramount, it nonetheless recognized an existing informational privacy interest when the information is compiled in computerized records. The Court stated:

We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. In some circumstances that duty arguably has its roots in the Constitution.

The Court’s recognition that computerized data banks can invoke unique privacy concerns shows that, while there may not be an absolute right of informational privacy, neither is there an unyielding rule favoring disclosure. Special circumstances, such as the method of

134. Id.
135. See id. at 597-98.
136. Id.
137. See infra Part III.B (discussing “fair information practices” and their requirements for responsible data collection and usage).
138. Whalen, 429 U.S. at 605.
139. Id. (footnotes omitted); see also id. at 606 (Brennan, J., concurring) (“Broad dissemination by state officials of such information, however, would clearly implicate constitutionally protected privacy rights . . .”).
140. Brennan highlights this concern in his concurrence. He states:

[T]he Constitution puts limits not only on the types of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential
information collection and dissemination, may have to be considered in weighing whether certain information should or should not be accumulated and disseminated.

Cases following Whalen have been reluctant to protect plaintiffs’ informational privacy interests against government disclosure, finding that the government’s need to collect and disseminate outweighs the plaintiffs’ privacy interest.141 Whalen’s progeny, while ultimately finding in favor of information dissemination, have still not obliterated the individual’s privacy interests. For example, one line of cases following Whalen holds that the press has a right to publish information lawfully obtained from government records, even though such publication may threaten an individual’s privacy interests.142 In Florida Star v. B.J.F.,143 for example, the Court held that the State could not punish or abridge the press’s First Amendment right to publish a rape victim’s name when obtained from a publicly released police report.144 The Court limited its holding, however, to cases where the action lay against the press and did not consider the extent to which the government could ever protect individuals from such disclosures.145

This Note does not debate whether the press can freely publish information obtained from state data banks—the case law shows it can. Rather, it considers whether, if the information must be collected, physicians have a right to oversee and limit the dissemination of this information in the first place.146 The decisions affirming the press’s right to publish information lawfully obtained from government data for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.

Id. at 607 (Brennan, J., concurring).


142. Florida Star v. B.J.F., 491 U.S. 524 (1989) (finding it unconstitutional to limit the press’s right to publish a rape victim’s name where the government inadvertently provided this information); Smith v. Daily Mail Publ’g Co., 443 U.S. 97 (1979) (holding it unconstitutional to sanction the press for publishing the name of a juvenile charged with murder); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975) (finding that the press had a right to publish a rape victim's name obtained from public judicial records).


144. Id. at 541.

145. Id. (“Our holding today is limited. We do not hold that truthful publication is automatically constitutionally protected, or that there is no zone of personal privacy within which the State may protect the individual from intrusion by the press . . . .”).

146. A competing concern is that, because the information is collected by the government and not private parties, the public has a right of access based on the Freedom of Information Act, 5 U.S.C. § 552 (1994). This Note points out, however, that the Freedom of Information Act is inapplicable to the National Practitioner Data Bank. See infra notes 251-56 and accompanying text (discussing the inapplicability of FOIA based on exception and the “central purpose doctrine”).
banks have also reaffirmed the government's responsibility to maintain the security of confidential or private information.\textsuperscript{147} Therefore, while it is unclear the extent of physicians' constitutional right to prohibit the dissemination of information about them obtained from information data banks, United States Supreme Court case law demonstrates that they nonetheless have an interest in how the information that they are compelled to disclose is treated.\textsuperscript{148}

4. Traditional Torts Framework as a Model for Defining a Physician Privacy Interest

Although it is clear that physicians do not have a fundamental Constitutional right to prohibit the collection or dissemination of this information, they still retain a privacy interest in the information. At present, however, the law is not clear exactly what this privacy interest is. One way this Note attempts to define the physician's privacy interest in the information that currently is or may potentially be collected in physician data banks is by looking to the values inherent in the traditional privacy torts framework. Because here it is the government that is collecting the physician information and not a private party, the privacy torts clearly would not provide physicians claiming a privacy violation with any sort of judicial redress.\textsuperscript{149} What these torts can do, however, is provide a framework of privacy values that can be extrapolated and applied here to define the extent of the privacy interest that physicians do have and to help determine what can be done to protect it.\textsuperscript{150}

\textsuperscript{147} Florida Star, 491 U.S. at 534 ("The government may classify certain information, establish and enforce procedures ensuring its redacted release . . . ."); Cox Broad., 420 U.S. at 496.

If there are privacy interests to be protected in judicial proceedings, the States must respond by means which avoid public documentation or other exposure of private information. Their political institutions must weigh the interests in privacy with the interests of the public to know and of the press to publish.

\textit{Id.} Also, in finding that the compilation of drug prescription records did not violate privacy rights, \textit{Whalen} focused, in part, on the security and confidentiality of the data bank. \textit{Whalen v. Roe}, 429 U.S. 589, 594-95 (1977).

148. Ironically, the fact that the courts have given the press such a broad right to publish lawfully-obtained government information may actually bolster the argument that the government bears a responsibility for the information it collects. The subsequent uses sanctioned by the court, while exemplative of freedom of speech ideals, are arguably not always the type of speech that society most wants to protect. \textit{See, e.g.}, Innovative Database Sys. v. Morales, 990 F.2d 217 (1993) (declaring unconstitutional a Texas law prohibiting the dissemination of government crime and motor vehicle accident reports for purposes of lawyer and chiropractor solicitations).

149. \textit{See infra} notes 153-62, 167-74 & accompanying text (discussing the torts of false light in the public eye and public dissemination of private facts and why they are inapplicable to physician privacy interests here).

150. \textit{See, e.g.}, Robert D. Sack & Sandra S. Baron, Libel, Slander, and Related Problems § 10.4.5.5, at 606 (2d ed. 1994) (discussing how two state courts used common law privacy principles to interpret privacy rights implicated by the government's collection and dissemination of information).
The foundation for the current torts privacy framework was established by Professor Prosser in his law review article, *Privacy*, in which he identified four privacy torts that subsequently have been adopted in some form or amount by almost all fifty states. The two torts most applicable here are (a) public disclosure of private facts, and (b) false light in the public eye.

### a. The Public Disclosure of Private Facts Tort

The tort of public disclosure of private facts provides a cause of action for the invasion of an individual's privacy if "the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." Putting aside the fact that a physician's complaint here would be against the government and not a private party, a physician still could not satisfy the requisite elements to bring a cause of action for public disclosure of private facts based on dissemination of physician data bank information. For this tort to apply, the disseminated information must be (a) disseminated to the public; (b) identifiable as pertaining to the plaintiff; (c) private; (d) offensive to a person of ordinary sensibilities; and (e) not of legitimate public interest.

Although the information contained in physician data banks is sometimes available to the general public and identifies the physician, it is clearly not offensive to a person of ordinary sensibilities. The element most absent here is the requirement that the information at issue be "private." First, some of the information contained in physician data banks, such as malpractice judgments and licensing actions, is already available through other public sources, such as courthouse records, state medical board records, etc. Dissemination of this information would therefore be non-actionable under the public disclosure of private facts torts. More damaging to the physician's privacy interest, however, is the argument that the remainder of the information at issue is not personal, but business, information and thus subject to a much lower level of privacy protection. Some have

---

151. William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960). Prosser's four privacy torts are included in the Restatement (Second) of Torts as (a) public disclosure of private facts, (b) appropriation, (c) intrusion upon physical solitude or seclusion, and (d) false light in the public eye. Restatement (Second) of Torts § 652A (1977).
155. *See infra* notes 303-04 and accompanying text.
156. "There is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public." Restatement (Second) of Torts § 652D cmt. b (1977); *see also* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 494-95 (1975) (holding that where the information is public a right of dissemination exists).
argued that when information concerns business activities, the public's interest in obtaining relevant information about the product or service they wish to purchase and the business that supplies it is much stronger and the business's privacy interest much weaker.158 Based on this argument, the remainder of physician information would be unprotected—both under the public dissemination of private facts tort and general privacy protection principles.159

In addition, to prevail a plaintiff must also prove that the information at issue is not of legitimate public interest or "newsworthy."160 At least one case has held that information related to the public's interest in policing its physicians is newsworthy and of legitimate concern to the public.161 Also, the courts have found that the tort does not apply to public information because "[w]hen the subject-matter of the publicity is of legitimate public concern, there is no invasion of privacy."162 Proponents of opening the data bank to the public argue that much of the information to which they desire access is already publicly available through courthouse and other government records, just not in so convenient a forum as a data bank would provide.163

A principle derived from this tort is that information should not be disseminated if it is not "of legitimate concern to the public." Some of the information currently contained in the National Practitioner Data Bank and other state data banks, while helpful for the purposes of peer review, is not of legitimate concern to the general public.164 While the public desires access to the information in the data banks to protection to entities doing business with the public, thus restricting the public's interest in a free flow of information).

In the United State, it is clear that collecting and disseminating business information that includes data about individuals does not automatically trigger rights in the individual. In principle, everyone is free to collect information from public and private non confidential sources and to use it to comment on the business activities of one's neighbors.

Id. at 626.
158. Id. at 620.
159. This does not mean, however, that physicians have no right in the protection of this information. While physicians are professionals, they are not absolutely akin to business corporations. Although the information at issue concerns a physician's professional abilities, it also directly concerns his personal reputation and private life.
160. See, e.g., Ayash v. Dana Farber Cancer Inst., No. CIV.A. 96-0565-E, 1997 WL 438769, at *5 (July 9, 1997) (defining the test for newsworthiness as whether "(a) the general matter at issue is one that is typically of public concern, and (b) the private facts disclosed are closely related to that matter of public concern.").
161. See Gilbert v. Medical Econs. Co., 665 F.2d 305, 309 (10th Cir. 1981) (finding that policing of the medical profession is newsworthy); Ayash, 1997 WL at *6 ("Deficiencies in health care are generally a matter of public concern.").
163. See Margolis, supra note 41, at 25 (discussing the difficulty of obtaining this information independently).
164. The best example is malpractice settlement payments. While they may help peer review boards target potential problems, their ability to predict future incompetence by a physicians is the subject of great dispute. See supra notes 327-37 and accompanying text.
help it identify and avoid negligent practitioners, it has not been es-
established that the data bank information actually meets this goal.\textsuperscript{165} Some of the information contained in the data banks is not evidence of a doctor's ability to practice medicine, and even the information that is evidence of past malpractice, such as malpractice judgments and settlement payments, may not actually be able to predict which doctors are truly incompetent and whether they will commit malprac-
tice in the future.\textsuperscript{166}

For this reason, the AMA is opposed to including any physician malpractice payments in the National Practitioner Data Bank,\textsuperscript{167} and argues that if malpractice payments must be included, only amounts over $30,000 should be included.\textsuperscript{168} The $30,000 threshold is based on the assumption that amounts below $30,000 indicate the settlement of frivolous suits, which are less likely to help patients identify incompetent practitioners.\textsuperscript{169} If the public is given open access, physicians are asked to sacrifice personal information, not to serve a legitimate public need, but to satisfy a baseless public curiosity.\textsuperscript{170}

\textsuperscript{165} This is not to say that the information contained in the physician data banks has no predictive value. In fact, insurers maintain data banks of much of this same information for the purposes of calculating risk. See, e.g., W. John Thomas, \textit{The Medical Malpractice “Crisis”: A Critical Examination of a Public Debate}, 65 Temple L. Rev. 459, 477 (citing to the Insurance Service Office, which is the “central rating bureau for the liability insurance industry [that] collects data from member companies, identifies and projects trends in liability claims, and computes advisory premiums for its members” to determine whether insurers' malpractice data truly reflects a “malpractice crisis”). There is a difference, however, between calculating whether a physician is going to be sued again and the likelihood that a physician will commit future malpractice. See infra notes 326-336 and accompanying text (discussing how studies have differentiated between the two). With regard to malpractice rates, for example, the factors that make a physician amenable to suit are not necessarily the factors that make him an incompetent practitioner. See Wendy Levinson et. al., \textit{Physician-Patient Communication: The Relationship with Malpractice Claims Among Primary Care Physicians and Surgeons}, JAMA, Feb 19, 1997, at 553 (discussing factors besides incompetence that put physicians at risk for a lawsuit).

\textsuperscript{166} For further discussion on the types of information that should and should not be included in a data bank protective of physician privacy, see infra part IV.B.4. Part IV provides an ideal data bank and discusses the types of information that should be disseminated in order to best meet medical consumer's informational needs while still protecting physician privacy.

\textsuperscript{167} AMA Pol'y Compendium ¶ 355.985 (1996).

\textsuperscript{168} Id. ¶ 355.993(6).

\textsuperscript{169} See infra note 327 (discussing how a $30,000 limit might eliminate the inclusion of frivolous malpractice suits); see also Ryzen, \textit{supra} note 76, at 450 (proposing that only malpractice payments over $30,000 be included in the National Practitioner Data Bank).

\textsuperscript{170} Such information may mislead rather than enlighten consumers. See generally Bobinski, \textit{supra} note 73, at 330 (arguing against disclosure as a remedy to health care problems). "Disclosure duties are an imperfect answer to the problem of provider-associated risk because they (1) threaten the privacy interests of providers, and (2) are not clearly authorized under existing legal doctrines or are uncertain in scope and effect.” \textit{Id.}"
b. The False Light in the Public Eye Tort

Traditional tort law protects individuals from injury resulting from "false light exposure" by providing a cause of action against one who represents another to the public in a false light if "(a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed." For the false light tort to apply, the published material at issue must be: (a) public, (b) about the plaintiff, (c) unprivileged, (d) offensive, and (e) false. As with the tort of public disclosure of private facts, physicians are unable to bring a cause of action under this tort because it is doubtful that a court would consider the publication of this information as "highly offensive." In addition, the physician information here is true—an absolute defense to this tort. Furthermore, it is generally accepted that "unfairness, improper tone, and unfounded implication and innuendo" are insufficient to invoke the tort.

Nonetheless, from the false light tort is extractable the value that, even though an individual may not be able to protect the dissemination of the information itself, especially if it is already publicly available, he may still have a privacy interest in protecting how and for what purposes the information is conveyed. Individual facts, although singularly true, may create a false representation, or "false light," when combined with other facts and disseminated for certain purposes. This privacy concern is implicated by the availability of physician profiles in data banks because specific pieces of information, such as a single malpractice payment or peer review investigation, may

171. Restatement (Second) of Torts § 652E (1977); see, e.g., Douglass v. Hustler Magazine, Inc., 769 F.2d 1128, 1135-38 (7th Cir. 1985) (holding that Hustler's publication of a nude picture in which plaintiff voluntarily posed for Playboy, but not Hustler, could mislead people to think plaintiff was the type of person who would pose for Hustler); Gill v. Curtis Publ'g Co., 239 P.2d 630, 632-35 (Cal. 1952) (finding that a picture of a moral, upstanding couple embracing, which accompanied an article on how sexual attraction leads to divorce, violated the plaintiffs' privacy rights by making it seem like they engaged in that type of relationship).

172. Sack & Baron, supra note 150, § 10.3.1, at 563 (2d ed. 1994) (presenting the elements of the false light in the public eye tort).

173. In addition, the false light tort generally redresses damages to a person's feelings—not reputation. Id. § 10.3, at 562.

174. Id. at 564.

175. Id. at 565.

176. The rationale for the false light tort is to prevent the corruption of a person's image by the dissemination of information in a form or compilation that is "misleading" in the representation such dissemination creates. Setting Standards, supra note 118, at 505. "The minimalist restraint on misappropriation of personal information and the narrow 'false light' protection strive to harness the circulation of deceptive information that may manipulate citizens' perceptions of each other." Id. at 507.
not actually indicate incompetence on the physician’s part.\textsuperscript{177} When they are placed together in an electronic data bank that can be accessed by anyone, however, they coalesce to take a form suggesting negligence.\textsuperscript{178} This is true even though the facts in the data bank, taken individually, may not necessarily be evidence of incompetence.\textsuperscript{179} The mere fact that this data is being compiled for the purpose of allowing consumers to identify negligent practitioners creates a presumption that any information contained in the data bank is evidence of malpractice.

\textbf{B. Informational Privacy in the Information Age—The Need for “Fair Information Practices”}

Physicians’ privacy interests are further compromised here by the compilation and dissemination of the physician information in electronic data banks that are accessible through the Internet.\textsuperscript{180} This section discusses the unique privacy interests that must be considered whenever information is contained in and disseminated from an electronic data bank. This section also introduces “fair information practices,” precautions and safeguards that should be implemented in order to protect these unique privacy interests.

1. Unique Privacy Concerns Invoked by the Accumulation and Dissemination of Sensitive Information in an Electronic Format

In identifying privacy interests, Brandeis and Warren were not oblivious to the effect of change on the definition of privacy.\textsuperscript{181} In their seminal article, they stated:

\begin{quote}
That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.\textsuperscript{182}
\end{quote}

\textsuperscript{177} For example, with regard to settlement payments, the National Practitioner Data Bank regulations specifically state that “[a] payment in settlement of a medical malpractice action or claim shall not be construed as creating a presumption that medical malpractice has occurred.” National Practitioner Data Bank for Adverse Information on Physicians and Other Health Care Practitioners, 45 C.F.R. § 60.7(d) (1996).

\textsuperscript{178} For example, evidence of multiple malpractice settlements together may jointly create an appearance that a physician is incompetent, even though each individual payment was made to settle a nuisance suit not proven to be the result of actual malpractice. See infra note 327.

\textsuperscript{179} See infra Part IV.B.4.e.

\textsuperscript{180} See supra note 62 and accompanying text (discussing how the Massachusetts data bank is now accessible on the Internet).

\textsuperscript{181} Warren & Brandeis, supra note 117, at 193.

\textsuperscript{182} Id.
While providing citizens with more information and thus helping ensure a more enlightened citizenry, the use of computer data banks and online access to these data banks have created new and unique privacy concerns that, in and of themselves, present a great threat to society.\footnote{183} Otherwise innocuous information may present an insidious threat when compiled with other information in a data bank or when made available for mass electronic dissemination.\footnote{184} Failure to implement fair information practices erodes general confidence in the security of the network and, consequently, in the network itself.\footnote{185} When the medical community loses faith in the security of information contained in physician databases, physicians and the peer review boards they comprise will be less willing to report data to and request information from physician data banks,\footnote{186} which in turn diminishes the effectiveness of peer review and health care in general.\footnote{187}

\footnote{183} Joel R. Reidenberg & Francoise Gamet-Pol, The Fundamental Role of Privacy and Confidence in the Network, 30 Wake Forest L. Rev. 105, 107 (1995) [hereinafter Fundamental Role] ("While networks may bring great benefits to society, they may also give rise to social costs associated with the use of personal information."); see also Dennis Campbell & Joy Fisher, Data Transmission and Privacy 501 (1994) ("The access and dissemination of data in the age of electronics takes on new, and for many, frightening proportions."); Dorothy E. Denning & Herbert S. Lin, Rights and Responsibilities of Participants in Networked Communities 113-19 (1994) (discussing reoccurring concerns with protecting the information in electronic networks); Graham, supra note 118, at 1395, 1402 ("The ‘information age,’ characterized by the introduction of computers into every area of life, threatens individual privacy in ways that were unimaginable just a short time ago. . . [T]his loss of privacy is the most serious casualty of the information age."); Peck, supra note 76, at 900-01 ("The new capacity to store and retrieve information has not so much redefined privacy as it has enhanced its importance.").

\footnote{184} Some have stated that it is not the processing of information, but its dissemination that is harmful. Chlapowski, supra note 120, at 133-34; Graham, supra note 118, at 1429. Arguably, there is a legitimate purpose in compiling physician information in data banks like the National Practitioner Data Bank. Doing so raises the general quality of health care by improving peer review and allowing licensing boards to more easily identify incompetent physicians. See supra Part II.A. Privacy violations nonetheless occur when this information is improperly monitored and indiscriminately disseminated to the wrong individuals.

\footnote{185} Fundamental Role, supra note 183, at 107 ("[P]ublic and private confidence is indispensable for robust networks to flourish, and such confidence, in turn, depends on the fair treatment of personal information.").

\footnote{186} See Ryzen, supra note 76, at 442-45 (discussing the psychological impact on physicians of being reported to the National Practitioner Data Bank even though this same information had previously been collected by government agencies). It is arguable that if the mere collection of physician information in a centralized data bank upsets physicians, their fears will only increase if that data bank is available to the general public.

\footnote{187} See supra Part II.B.2 (discussing the potential negative effects on peer review and overall health care that may result when physicians shun physician data banks out of fear for their reputation). One possible solution is to give those about whom information is being collected a larger role in determining how that information should be disseminated. See Denning & Lin, supra note 183, at 99-112. In this context, the American Medical Association could be given a larger voice, as an advocate for its physician members, on the types and manner in which information should be disseminated. The AMA already maintains its own Internet Web Page to provide physi-
Although fair information practices should apply to all data banks, they are particularly important when the information is available online or through the Internet,\textsuperscript{188} as is the case with the Massachusetts and other state data banks.\textsuperscript{189} When information is available on the Internet, it is more readily and easily accessible by more people than other methods of information dissemination. While there are benefits to placing physician information on the Internet, at present, there are inadequate safeguards for establishing and maintaining the integrity of this information.\textsuperscript{190}

2. Fair Information Practices

To better maintain the information's integrity, many legal scholars have advocated information processing systems that incorporate "fair information practices" to protect the unique privacy concerns surrounding electronic information dissemination.\textsuperscript{191} Professor Reidenberg defines "fair information practices" as "standards [that] apply to the collection, storage, use, and disclosure of personal information" in order to maintain "the integrity of personal information and fairness to the individuals about whom the data relates."\textsuperscript{192} Fair information practices take into account the effect of technology on personal information.\textsuperscript{193} Instead of searching for ways to remedy privacy abuses, fair information practices require that the government takes an active role in ensuring that the information it requires is collected, maintained, and disseminated in a responsible manner.\textsuperscript{194} Fair information practices proponents advocate applying certain principles to concrete models of data systems rather than forcing individuals to rely on a vague concept of privacy that may or may not protect their particular privacy interest.\textsuperscript{195}

\begin{footnotesize}
\textsuperscript{188} See Fundamental Role, supra note 183, at 119-20.

\textsuperscript{189} See supra notes 61-62 and accompanying text.

\textsuperscript{190} Fundamental Role, supra note 183, at 120-21 (discussing how, with regard to information on the Internet, quality measures have not improved commensurate with quantity).

\textsuperscript{191} See Campbell & Fisher, supra note 183, at 488; Gostin, supra note 121, at 25; Schwartz, supra note 125, at 323; Schwartz & Reidenberg, supra note 126, at 12-17; Setting Standards, supra note 118, at 498.

\textsuperscript{192} Setting Standards, supra note 118, at 498.

\textsuperscript{193} Id. at 323.

\textsuperscript{194} See Schwartz, supra note 125, at 323 (arguing that, because lost data privacy is never regained, the value of fair information practices is their ability to establish a set of proactive data protection regulations); see also Schwartz & Reidenberg, supra note 126, at 12-13 (discussing European use of fair information practices).

\textsuperscript{195} Schwartz, supra note 125, at 323. "[A]bstract, generally applicable provisions should be abandoned in favor of a context-bound allocation of information embodied in a complex system of both specific and substantive regulations." Id. (quoting Spiros Simitis, an international data protection expert).
\end{footnotesize}
Various legal scholars and government commissions have proposed frameworks to incorporate fair information practices in the electronic compilation and dissemination of information.\textsuperscript{196} While the components of these frameworks differ in terminology they all represent the same basic principles of privacy protection. For simplicity, this Note will use the terminology adopted by Professor Reidenberg\textsuperscript{197} in his call for the creation and implementation of U.S. data protection standards.\textsuperscript{198} Professor Reidenberg's model calls for: (a) data quality standards, (b) transparency in information processing, (c) enforcement mechanisms to ensure fair information practices, and (d) special protection of sensitive data.\textsuperscript{199}

a. \textit{Data Quality Standards}

The first step in utilizing fair information practices is to establish standards to guarantee data quality.\textsuperscript{200} According to Professor Reidenberg, "The benchmark of data quality consists of commonly accepted standards to assure that personal information is acquired legitimately and is used in a manner that treats fairly the interests of individuals, industry, and society."\textsuperscript{201} In interpreting what constitutes data quality, Professor Reidenberg has drawn common elements from various international data protection models that incorporate the qualities of: (1) fair and permissible uses, (2) relevancy, (3) timeliness, (4) accuracy, and (5) reliability.\textsuperscript{202} The first two criteria, fair and per-


\textsuperscript{197} \textit{Setting Standards}, \textit{supra} note 118, at 513-16.

\textsuperscript{198} \textit{Id.}; see also Campbell & Fisher, \textit{supra} note 183, at 488 (advocating a data systems protection model similar to Professor Reidenberg's).

Key elements of an individual's privacy rights as they relate to data transmission include the right to determine how personal information is used by others with protection against inappropriate use, openness and fairness in person's relationship with any organization maintaining data about him or her, including the right to know if personal data (what and where) are collected, stored, and disclosed; protection against unnecessary or excessive collection or dissemination of personal information; and protection against the interception, alteration, or destruction of personal information being transmitted electronically.

\textit{Id.}

\textsuperscript{199} \textit{Setting Standards}, \textit{supra} note 118, at 513-16.

\textsuperscript{200} Quality data is that which is collected only for specific purposes and used only in a manner compatible with those purposes. Schwartz & Reidenberg, \textit{supra} note 126, at 13-14. Furthermore, to ensure data quality, organizations should collect the minimum amount of information necessary to achieve their informational goals and take care to eliminate information that is no longer necessary. \textit{Id.} at 14-15.

\textsuperscript{201} \textit{Setting Standards}, \textit{supra} note 118, at 514.

\textsuperscript{202} \textit{Fundamental Role}, \textit{supra} note 183, at 110. Professors Reidenberg and Schwartz call for international data protection standards to protect U.S. involvement
missible uses and relevancy, require that the information collected be used "lawfully for specific purposes." The concept of data quality is similar to the common law privacy notion that dissemination of otherwise innocuous, non-violative information can nonetheless violate an individual's privacy rights where the information disseminated exceeds the public's legitimate use for that information.

In addition, quality data is that which is timely for its uses. After a certain time period, data no longer represents the same proposition it once did. Also, additional measures should be installed by those maintaining the physician data banks to ensure they are regularly monitored for accuracy and reliability.

Another key element to ensuring high quality data is to stop secondary use of the data beyond that for which it was initially collected and disclosed. Even though the information disclosed in one data bank may not violate a privacy interest, that information re-compiled in a different format may give the information a new character—create a sort of "false light" interest—and therefore affect the person's privacy interest in the international marketplace; they adopt their standards, in part, from European data protection proposals such as the Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing Personal Data and on the Free Movement of Such Data, Econ. Comm. Doc. COM (92) 422, 54N 287, art. 6(1)(b) (Oct. 15, 1992). See Schwartz & Reidenberg, supra note 126, at 31-36 (defining fair information practices based on European data protection principles); see also Schwartz, supra note 125, at 324-33 (also looking to the European standards for guidance in establishing a data protection standard incorporating fair information practices).

203. Setting Standards, supra note 118, at 514.

204. Professor Schwartz, in advocating the privacy rights of patients in their own medical records, recognizes that while there are numerous legitimate uses for the collection and disclosure of patient data, patients' privacy rights are compromised when use and disclosure exceed the legitimate use. Schwartz, supra note 125, at 334 ("Use of health care information should only be permitted for reasons that are compatible with the purpose for which the information was collected. The principle of compatibility requires a significant degree of convergence—a concrete relationship—between the purpose for which the information was gathered and its subsequent use."); see also Gostin, supra note 121, at 25 (arguing that "information should be collected only to the extent necessary to carry out the purpose for which the information is collected").

205. See Gostin, supra note 121, at 25 ("[I]nformation should be disposed of when no longer necessary to carry out the purpose for which it was collected 


207. Gostin, supra note 121, at 25.

208. Id. ("[I]nformation collected for one purpose should not be used for another purpose without the individual's informed consent 

209. This qualification implicates the rights protected by the false light privacy tort. Although the false light tort does not directly apply to the physician privacy interest...
privacy interest. As a result of such secondary usage, users lose control over sensitive information, and confidence in the network is consequently weakened. Physicians' privacy interests are clearly threatened when sensitive information is taken from their files and recompiled for illegitimate purposes.211

b. Standards for Transparency of Information Processing

Although fair information practices primarily require adopting measures to secure the integrity of protected data, they also meet societal concerns by ensuring the public the minimum necessary restriction on flows of information.212 One way to achieve this objective without compromising privacy interests is to provide for as transparent a system of information processing as possible.213 A "transparent" data system ensures that the data bank is open and understood by the public who may access it,214 and especially by those about whom information is included in the data bank.215 For example, transparency requires that those who may be profiled be told what information about them is being included and for what purpose.216 Individuals should know what record keeping practices exist.217 Ensuring transparency here, it represents the value of ensuring that the data not be used to misrepresent the information. See supra Part III.A.4.b (discussing the values inherent in Prosser's false light privacy tort and applying them to the physician privacy interest).

210. Professors Reidenberg and Gamet-Pol note that the electronic network in itself is a threat to this interest because the widespread access it provides increases opportunities for secondary usage to occur. Fundamental Role, supra note 183, at 112; see also Graham, supra note 118, at 1402-03 (discussing how the invasion of computers has increased the risk that personal information is used for other than its original purposes).

211. Such illegitimate purposes may include "trolling" by plaintiff's attorneys, Ryzen, supra note 76, at 456 n.238, or defaming a physician with a substance abuse or medical problem.

One way to prevent such nefarious uses is through end-use restrictions, which limit the purposes for which the information can be disseminated and place sanctions on unlawful secondary use of the information. For example, the AMA argues that information obtained from the National Practitioner Data Bank should not be given to any party who does not already have direct access to the National Practitioner Data Bank. AMA Pol'y Compendium ¶ 355.999(4) (1996).

212. Fundamental Role, supra note 183, at 109.

213. Setting Standards, supra note 118, at 515; Schwartz, supra note 125, at 336-37.


215. Schwartz, supra note 125, at 336. Professor Schwartz, in discussing the rights of medical patients with regards to their medical records, calls for "notice of information practices" that would provide individuals with a description of their rights and the procedures under which such rights could be exercised; a right of correction if the information is not timely, accurate, and complete; a reason for the collection of the particular information about the individual and by whom the information collected is going to be used; and the extent of disclosure. Id. at 336-37. Professor Schwartz maintains that "[o]nly this knowledge, provided by the notice requirement, would allow the individual to play a role in preventing collection, storage, and use of unnecessary information." Id. at 337.

216. Id.

217. Gostin, supra note 121, at 25.
in information processing also requires establishing procedures that allow individuals to check the information reported about them and a fair dispute resolution system in the event a conflict arises over the information's accuracy.\(^{218}\) In addition to meeting societal concerns, a transparent system better protects privacy because it gives the profiled individual more knowledge and control to ensure that the information is not wrongly reported or subsequently abused.

c. Enforcement of Fair Information Practices

Fair information practices lose their impact if they are not supported by meaningful enforcement measures. They require "supervision and oversight of the treatment of personal information."\(^{219}\) In addition, those in charge of such information should not only ensure its accuracy, but also adopt procedures to provide redress to those challenging the information's accuracy.\(^{220}\)

d. Special Protection for Sensitive Data

This requirement mandates a recognition that certain types of information—such as race, religion, criminal convictions, health, or political beliefs—are more sensitive and must be afforded a higher level of privacy protection.\(^{221}\) Fair information practices strictly limit sensitive information to these enumerated categories. This Note, however, expands this category. Drawing on the recognition, implicit in fair information practices sensitivity category, that certain types of information deserve different degrees of privacy protection, this Note attempts to categorize information into differing levels of dissemination based not only on the information that fair information practices labels as sensitive, but also on the information's ability to satisfy other fair information practices requirements, such as data quality.\(^{222}\)

C. Proactive Data Protection Model Based on Physicians' Privacy Interests

As Part III has shown, physicians do not have a clearly defined right to protect the information contained in federal and state physician data banks from being disseminated to the general public. A recurring theme running through the law's treatment of privacy has been the process of weighing the public's right to know information against

\(^{218}\) Id.

\(^{219}\) Setting Standards, supra note 118, at 515. See, e.g., Schwartz, supra note 125, at 341-42 (arguing for a United States Data Protection Board to serve as a "general privacy protection agency").

\(^{220}\) Setting Standards, supra note 118, at 515; Gostin, supra note 121, at 25.

\(^{221}\) Setting Standards, supra note 118, at 515.

\(^{222}\) See infra part IV.B.4 for a discussion of the types of physician information that should and should not be available to the general public.
the individual’s right of privacy. Considering physician data banks in the context of this traditional balancing test, the physician is likely to lose because the public’s strong right to make choices and calculate their own risk outweighs the physician’s ambiguous interest in maintaining the confidentiality of diverse types of public and private information.

The balancing test does not mean, however, that there is an absolute right to dissemination of all physician information. Professor Schwartz has argued that, in most cases, individuals’ privacy will lose out if data protection is considered as this all-or-nothing proposition between full disclosure and a “right to seclusion,” or right of an individual to withhold information from the public. To ensure data protection and the use of fair information practices, he instead advocates a model of “privacy as participation.” In this model, the question is not what personal information an individual can withhold, but how to monitor the collection and dissemination of information so as to encourage citizens to participate in the process, by ensuring that the “individual’s capacity for decisionmaking is respected and encouraged.”

Professor Schwartz’s model addresses the privacy balancing test by arguing that “[d]ata protection law in the computer age

223. In interpreting Whalen, several of the circuits have found that Whalen requires a balancing test of the individual’s right to privacy against the state’s reasons for compilation and disclosure. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577-80 (3d Cir. 1980); Plante v. Gonzalez, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978); see also Privacy and Participation, supra note 129, at 575 (“Whalen and its progeny reveal an American constitutional right of informational privacy that is suspended between privacy paradigms of participation and seclusion.”); Chlapowski, supra note 120, at 146 (noting that Whalen established the foundation for subsequent courts to find “another level of scrutiny in substantive due process analysis, one which focuses on a consideration and balance of public and private interests in legislation”). But see J.P. v. DeSanti, 653 F.2d 1080, 1088-89 (6th Cir. 1981) (discussing these cases and disagreeing with the balancing test).

Other commentators have agreed. See Freedman, supra note 118, at 11 (discussing the use of the balancing test with regard to patient information); see generally Gostin, supra note 121, at 17 (discussing how, in a health care setting, an individual’s privacy and autonomy must be balanced against society’s need for an efficient and safe health care system). “The balancing test requires the Court to weigh the state’s need to protect the general welfare through its police power against an individual’s right to prevent unnecessary governmental interference.” Grace K. Hogan & Nichole Wertz, Privacy, Privilege and the Right to Know: Disclosure of AIDS/HIV Status in the Physician-Patient Relationship, 11 St. John’s J. Legal Comment. 805, 811 (1996).

224. Privacy and Participation, supra note 129, at 558 (“[I]nformation seclusion is rarely achievable; when gathering personal information is the objective, good, perhaps even excellent, reasons will often exist not to leave someone alone.”). In the balancing context, “[p]rivacy as information seclusion tends to collapse in the face of the weighty reasons provided in support of seeking personal information.” Id. at 559.

225. See Privacy and Participation, supra note 129.

226. Id. at 555. “In the computer age, individual freedom cannot rest on a dream of being let alone by an ever-reduced government. Today, the safeguarding of liberty requires a legally structured pattern of access to and limitations on the use of personal information.” Id. at 618.
should respond by creating social patterns of access to and limitations on the use of personal information.”

Drawing on Professor Schwartz’s “privacy as participation” model, this Note argues that while physicians do not have a clear right to keep all information out of the public sphere, they nonetheless have an interest in protecting and governing how information about them is collected and used. They have an interest in ensuring the information is collected and disseminated responsibly and in conformity with fair information practices.

IV. A Proposal for a Federal Data Bank with Limited Public Access

Acknowledging that medical consumers have a legitimate right to conduct their own risk calculations in choosing physicians and drawing on Professor Schwartz’s model of “privacy as participation,” this Note presents a model physician data bank meant to satisfy the competing interests of both medical consumers and physicians, and ultimately to work towards improving health care. This part advocates amending the HCQIA and the National Practitioner Data Bank regulations to provide the public limited access to the National Practitioner Data Bank and to reflect the importance of fair information practices in ensuring physician privacy.

To arrive at this solution, this part first examines the different standards of privacy protection among the several states and between the states and the federal government, and considers the interstate commerce problems created by multifarious state data banks, which undermine the privacy protections that the Freedom of Information Act and the Privacy Act have already imposed on the National Practitioner Data Bank. This Note determines that a federal data bank best avoids such problems. Taking into consideration the reforms advocated by the American Medical Association, this part then argues that the guidelines for the proposed federal data bank should improve upon the standards established in setting up the National Practitioner Data Bank to fully incorporate fair information practices. Finally, following up on the privacy values inherent in common law traditions of privacy and fair information practices, this Note examines the types of information that either are or may potentially be contained in and disseminated from physician data banks, and determines which types of information should be disseminated and which should not. This limited dissemination, wherein medical consumers receive the information they need to assess risk, yet physicians maintain confidentiality of misleading and more “sensitive” information, will, in the long run, have the most positive effect on the overall quality of health care. This Note concludes that a federal data bank with limited public dis-

227. Id. at 616.
closure will provide medical consumers with the information they need to make prudent decisions, thus alleviating the need for state data banks that provide indiscriminate and, ultimately, privacy-violative information.\textsuperscript{228}

A. A Federal Remedy

1. Differences Between the States in Privacy Protections

States differ dramatically in the consideration given privacy interests.\textsuperscript{229} In particular, protection for informational privacy rights differs from state to state.\textsuperscript{230} This inconsistency, standing alone, is a threat to privacy\textsuperscript{231} because, in an age where information can instantaneously travel across state borders, an individual’s privacy right in any state is only as strong as that of the state offering the least privacy protections.\textsuperscript{232} The states’ lack of privacy protection for their citizens is a strong rationale for a federal remedy.\textsuperscript{233}

Because states have diverse views of informational privacy, it is not surprising that they disagree over what physician information should

\textsuperscript{228} This Note does not, however, argue for legislation prohibiting state data banks or limiting their exercise. To do so without a fundamental right to physician privacy would invoke federalism problems because the right to regulate physicians is a traditional state power. James F. Blumstein, \textit{A Perspective on Federalism and Medical Malpractice}, 14 Yale J. on Reg. 411, 412-13 (1996) (discussing how areas of medical malpractice and medical licensing are traditionally areas of state concern). But see Robert M. Gellman, \textit{Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules}, 41 Vill. L. Rev., 129, 138-39 (1996) (arguing that health care is interstate business).

At the same time, this Note does point out that, while the existence of a federal data bank does not compromise states’ interests, various state data banks giving access to information that the federal government has mandated should be private undermines the security and efficacy of the federal data bank. Ultimately, states should not need to create their own data banks once limited access to the National Practitioner Data Bank is provided.

\textsuperscript{229} See Campbell & Fisher, supra note 183, at 499 (“Some states have virtually no privacy laws, while others, such as California, have incorporated the right of privacy into the State Constitution.”); Bruce D. Goldstein, \textit{Confidentiality and Dissemination of Personal Information: An Examination of State Laws Governing Data Protection}, 41 Emory L.J. 1185, 1210 n.144 (1992) (providing case law to demonstrate the varying classifications of what qualifies as a privacy interest).

\textsuperscript{230} “State law that does exist represents a patchwork of inconsistent and inadequate protection of informational privacy.” Goldstein, supra note 121, at 8. “Some data protection exists in every state, but no two states have adopted precisely the same system of regulation.” \textit{Privacy and Participation}, supra note 129, at 604. Besides disagreeing as to what information collection violates privacy rights, “[s]tates also differ widely on how, when, and to whom protected data files may be released.” Goldstein, supra note 229, at 1198.

\textsuperscript{231} Goldstein, supra note 229, at 1194 (“The threat to individuals lies in the very diversity of standards.”); Schwartz, supra note 125, at 310.

\textsuperscript{232} Where informational privacy is concerned, even subtle differences in the way information is disseminated and what penalties will be imposed for wrongful promotion can effect an individual’s privacy rights. Goldstein, supra note 229, at 1195, 1198-1200, 1202.

\textsuperscript{233} Gostin, supra note 121, at 16-17.
be included in physician data banks and over what physician information should be disseminated to the public. This disparity, however, is inconsistent with one of the main goals of recording physician information in data banks—preventing incompetent physicians from committing malpractice or other prohibited behavior and then escaping liability by moving to another state that has no means of discovering their past behavior. If states have different requirements, a doctor with a nefarious past can hide past misdeeds by simply moving to a state that does not. Having physicians held to different standards of professional accountability is at odds with the national goal, as stated in the HCQIA, of improving the quality of health care nationwide.

2. Differences in Privacy Protections between the States and the Federal Government

In addition to state discrepancies over privacy rights, there is a growing disparity between the states and the federal government concerning citizens’ informational privacy rights. At the federal level, two main statutes govern the government’s treatment of the personal information that it collects. The Freedom of Information Act, or “FOIA,” "structures third-party access to federal records" and includes exceptions for the privacy of certain types of information. The Privacy Act of 1974 is an “omnibus data protection measure that regulates how federal agencies collect personal information and apply it in decisionmaking." These two statutes work together to govern the government’s treatment of personal information. These privacy protections, however, are not equally available at the state level. Although most states have some version of a FOIA statute, many of these statutes lack the privacy exemptions that the federal FOIA has. In addition, most states do not have a privacy statute

---

234. For example, while states such as Massachusetts release malpractice information, other states, such as Maryland, have laws to keep such information confidential. Maryland's Jaunt onto the Information Superhighway Hits Speed Bump, Rep. on Med. Guidelines & Outcomes Res., 1997 WL 8623929, *2 (Feb. 20, 1997), available in 1197 WL 8623929.
236. Id.
237. Id. § 11101.
238. Christopher P. Beall, The Exaltation of Privacy Doctrines over Public Information Law, 45 Duke L.J. 1249, 1252 (1996). Some have stated that this gap appears to be widening. Id.
240. Privacy and Participation, supra note 129, at 583.
243. See id. at 593-95 (discussing the interrelationship between the two statutes).
244. See id. at 605.
The weaknesses of state data protection law are heightened by the effect of state-level Freedom of Information Acts (FOIA). All states have statutes that regulate public access to governmental records; only some of these laws
equivalent to the Privacy Act. Because the Privacy Act contains many protections similar to fair information practices, the absence of a Privacy Act state equivalent has a harmful effect on the quality of data protection at the state level. The privacy statutes that do exist at the state level are often either overly broad or narrowly tailored to specific types of information.

In interpreting state statutes, courts have likewise favored disclosure over the protection of privacy. At the same time, the recent trend in federal case law has been to interpret Federal access statutes extremely narrowly so as to insulate privacy rights. For example, FOIA is the main authority for citizens to gain access to government records. In the past few years, however, despite the proclamation that FOIA is to be construed in favor of disclosure, citizens have encountered increasing difficulties in gaining access because courts have strictly construed FOIA and applied the central purpose doctrine. The "central purpose doctrine" holds that the "central purpose of FOIA is to provide the public with a means to monitor government activity and that any information that does not fulfill this purpose is exempt and should not be disclosed." For example, in United States Department of Justice v. Reporters Committee for Freedom of the Press, the Supreme Court held that when the informa-

---

245. Id. at 566 ("Most states lack laws, similar to the Privacy Act, that regulate the governmental use of personal information.").
246. Id. at 603-05 (discussing how, without state laws similar to the federal Privacy Act, state law lacks critical fair information practices).
247. See generally Beall, supra note 238, at 1252, 1284-95 (1996); Peck, supra note 76, at 897 nn.25-26 (providing a description of broad state statutes and citing certain narrowly-interpreted privacy rights that states have chosen to protect).
248. See, e.g., Gilbert v. Medical Econcs. Co., 665 F.2d 305, 306-07 (10th Cir. 1981) (upholding a Colorado court decision that the public's legitimate concern with the fitness of its professionals outweighed a physician's privacy interest in keeping her name, photograph, psychiatric history, and marital problems out of a magazine article); Kees v. Medical Bd. of Cal., 10 Cal. Rptr.2d 112, 119 (Cal. App. 4th 1992) (finding a statute authorizing the Board to order an impaired physician to undergo a mental exam did not violate the physician's privacy rights); State Bd. of Med. Exam'rs v. Fenwick Hall, 419 S.E.2d 222, 224 (S.C. 1992) (holding that the public's need to know of a physician's past drug abuse outweighed a threat to a physician's privacy); see also Beall, supra note 238, at 1295 ("Some states recently have taken a substantially more expansive approach to the recurring struggles between disclosure and privacy than the federal courts.").
249. See, e.g., Durham v. United States Dep't of Justice, 829 F. Supp. 428, 433 (D.D.C. 1993) ("[T]he goal of FOIA is to permit the public to scrutinize the activities of government; it is not intended to foster the dissemination of information gathered by the government about private citizens for the use of other citizens.").
251. Beall, supra note 238, at 1252, 1255-58.
252. Id. at 1258.
tion requested is not a record of the government's activities, the privacy interest is at its apex. The National Practitioner Data Bank's contents are the government's collection of information on physician performance and do not contain information on how the government itself is operating. Therefore, based on the recent interpretation of the central purpose doctrine, it is likely that courts would find the contents of the National Practitioner Data Bank also immune from FOIA's provisions.

The federal-state split over the amount of informational privacy afforded individuals mirrors the debate over whether physician data collected in government data banks should be available to the public in the first place. Despite numerous challenges, Congress has, thus far, refused to make public the contents of the National Practitioner Data Bank. At the same time, the same physician information contained in the National Practitioner Data Bank will become increasingly available, compromising the National Practitioner Data Bank, if more and more states follow Massachusetts and open to the public state depositories of physician information, which contain much of the same information that is kept confidential by the National Practitioner Data Bank.

3. A Federal Data Bank Solution

Because the overriding goal is the uniform improvement in health care, one way to accomplish this is by allowing the public access to a federal data bank governed by federal laws managing the treatment of

254. Id. at 780.


257. See supra notes 44-50 and accompanying text (describing Congressional efforts to publicize the National Practitioner Data Bank contents).

258. HCQIA, 42 U.S.C. § 11137(b) (1994); National Practitioner Data Bank for Adverse Information on Physicians and Other Health Care Practitioners, 45 C.F.R. § 60.13 (1996).
government information. While the states provide both dissemination and privacy protection indiscriminately and unevenly, applying federal statutes would ensure that a physician in Maine has the same amount of privacy protection as a physician in Oregon, and a potential patient in New York has the ability to obtain the same amount of information about her doctor as a potential patient in California. Limited access to the National Practitioner Data Bank better protects physician privacy interests than state data banks because a federal data bank invokes the regulations and requirements of various federal statutes, including the Freedom of Information Act and the Privacy Act, that have been established to guide administrators in weighing the public's need for information against the information subject's privacy interest. For example, FOIA reassures citizens of their democratic right to receive information concerning their government's activities—information that their status as citizens affords them—while the Privacy Act is Congress's attempt to reaffirm privacy rights and, therefore, grants certain protections to those whose privacy is being threatened.

The Privacy Act recognizes the government's legitimate need to collect information, sometimes even personal information, from private citizens; yet it also acknowledges the potential for harm should the government's ability to do so be abused. Congress thus enacted the Privacy Act to ensure the accuracy of the information the government collects, to protect personal and private information from unauthorized disclosure, and to bolster the privacy protections afforded individuals under the FOIA exemptions.

Because the Privacy Act specifically addresses privacy concerns involving personal information collected in government data banks, it is not surprising that many of its requirements are similar to those advocated as "fair information practices." For example, to ensure "data quality," the Privacy Act limits collection to only that information

259. See supra Part IV.A.1.
261. Harrison, supra note 118, at 778 ("Congress has statutorily acknowledged the right of the citizen to control publication of personal/private information about himself via the 'privacy exemptions' of the Freedom of Information Act and the Privacy Act.").
262. Id. at 782.
263. Id.
264. Id. at 786. The two are meant to be read together. FOIA cannot mandate disclosure of information that the Privacy Act makes exempt. FOIA, 5 U.S.C. § 552, n.10 (1994).
265. See supra Part III.B.2 (defining and discussing fair information practices).
266. See supra Part III.B.2.a.
relevant to the purpose for which such information is being compiled. Also, the Privacy Act seeks to ensure that the information contained in government data banks is accurate, relevant, timely, and complete. In order to protect against improper secondary data uses, the Privacy Act requires that information subjects be informed when information about them is being disseminated. The Privacy Act also features transparency requirements similar to those advocated by fair information practices.

The hallmark of the Privacy Act is its requirement that information subjects have access to their own records. This requirement, analogous to the data quality category of the fair information practices paradigm, provides for detailed procedures to allow an individual to contest and amend his report. Although some scholars have criticized the Privacy Act as failing to fully incorporate fair information practices, at present, the Privacy Act and FOIA provide a starting point for standards that must be employed when the government collects and disseminates information about citizens, and which can be improved upon by the full application of fair information practices and applied to a federal physician data bank that provides physician information through an electronic medium.

268. Id. §§ 552a(e)(5), 552a(e)(6).
269. See supra notes 208-11 and accompanying text.
270. 5 U.S.C. § 552a(e)(3). Section 552a(e)(10) requires that safeguards be established to protect the security of information that is designated confidential.
271. According to the Privacy Act, any agency that maintains a system of records must tell individuals from whom it requests information its authority for requesting the information and whether the disclosure is voluntary or mandatory, the purpose for which the information is to be used, the routine uses of the information, and the consequences should the individual fail to supply the required information. 5 U.S.C. § 552a(e)(3).

These requirements, however, are less effective when applied to physician data banks. Although the Privacy Act mandates that agencies obtain this information directly from the subject whenever possible, id. § 552a(e)(2), here third parties, not the physicians themselves, report the information to the government. One way the transparency requirement reemerges in the Privacy Act is the Act’s requirement that routine uses of information be disclosed in the Federal Register. Id. § 552a(e)(4)(d). Although individuals are less likely to read the Federal Register, the Privacy Act nonetheless provides a source for physicians to learn to what use information about them is put.

272. 5 U.S.C. § 552a(d); see also Harrison, supra note 118, at 793.
273. See supra Part III.B.2.d.
274. 5 U.S.C. § 552a(d)(1)-(3).
275. See Privacy and Participation, supra note 129, at 566-84 (arguing that the routine use exception and computer matching limit the Privacy Act’s ability to ensure data quality). But see James Rule et al., The Politics of Privacy 101-03 (1980); NPDB Fact Sheet, supra note 17 (stating how the Privacy Act protects the confidentiality of the National Practitioner Data Bank).
276. See Privacy and Participation, supra note 129, at 566 (arguing that the Privacy Act provides a better foundation for fair information practices than disparate state laws).
B. The Proposed Data Bank Should Incorporate Fair Information Practices

While many of the privacy protections mandated by the Privacy Act and FOIA exceptions and included in Professor Reidenberg and others' models are lacking or not readily apparent in the state data banks,\textsuperscript{277} they are already included, to a certain extent, in the legislation establishing the National Practitioner Data Bank. For example, consistent with data quality,\textsuperscript{278} the HCQIA provides for the information collected about a physician to be disclosed to that practitioner,\textsuperscript{279} and requires procedures for a physician to dispute the accuracy of the information.\textsuperscript{280} There are, however, many areas of data protection still lacking. This Note, therefore, argues that the HCQIA and the regulations for the National Practitioner Data Bank should be amended to ensure that the proposed, partially-open National Practitioner Data Bank contains additional privacy protections based on fair information practices. One source of these additional privacy protections is suggested in the American Medical Association's Policy Compendium, which presents the AMA's goals for a National Practitioner Data Bank more protective of physician interests.\textsuperscript{281} This Note considers the National Practitioner Data Bank regulations and the AMA's suggestions concerning the fair information practices categories: (1) data quality, (2) data transparency, (3) enforcement mechanisms, and (4) special protections for sensitive data.\textsuperscript{282}

1. Data Quality

Fair information practices mandate that information collected and maintained in electronic databases such as the proposed physician data bank be checked for relevancy, accuracy, and timeliness.\textsuperscript{283} Although the Federation of State Medical Boards recognizes the importance of providing consumers with information about negligent physicians, it has traditionally resisted making the National Practitioner Data Bank available to the public because of concerns about the quality of the information and its relevancy to the general public.\textsuperscript{284}

\textsuperscript{277} See supra notes 244-47 and accompanying text.
\textsuperscript{278} See supra Part III.B.2.a.
\textsuperscript{280} Id. § 11136(2).
\textsuperscript{281} AMA Pol'y Compendium ¶ 355.000 (1996). The AMA has traditionally called for the complete eradication of the National Practitioner Data Bank. AMA Pol'y Compendium ¶ 355.991 (amended res. 828, I-91). At the same time, the AMA calls for standards to secure physicians' privacy protections within the existing Data Bank.
\textsuperscript{282} This section will be discussed infra Part IV.B.4 where this Note proposes the types of information to which the public should have access.
\textsuperscript{283} See supra Part III.B.2.a.
\textsuperscript{284} "Our concern is not whether [the National Practitioner Data Bank] should be made public, . . . but that it's quality information." Jan Greene, Getting the Lowdown
In conformity with the Privacy Act framework, the National Practitioner Data Bank guidelines control who has access to the information and limit the purposes for which the information is used and disseminated. One way to ensure that disseminated information is relevant is to include in the amended statute end use restrictions that specifically state to whom the information can be disseminated and the limited purpose for which the information can be used (to choose physicians). This Note advocates specific statutory end use restrictions to prohibit and even impose punishment for those who wrongfully use the information or further disseminate it to secondary parties. For example, the AMA Policy Compendium calls for assurances that information taken from the National Practitioner Data Bank is used only for those purposes consistent with the rationale of the Health Care Quality Improvement Act and is not abused through wrongful secondary uses. In addition, in order to ensure information is timely, the AMA has advocated that information in the National Practitioner Data Bank be "purged" after five years.

2. Transparency

The transparency requirement of fair information practices mandates that individuals, especially those about whom information is being included in a data bank, know that information about them is being collected or disseminated and the reasons why such collection and dissemination is occurring. The AMA, in addition to its own educational initiatives, advocates alerting physicians to the existence of the National Practitioner Data Bank and the risk of broad dissemination of information reported to it. The AMA also advocates alerting physicians when their file has been queried.

285. See, e.g., 45 C.F.R. § 60.11 (1996) (discussing "[w]ho may request information and what information may be available"). Although this Note argues that the public should have more access than they currently have, the NPDB guidelines still place limits on who has access and to what information, as opposed to state systems following the Massachusetts model, which would apparently disclose information indiscriminately.

286. The HCQIA places an end use restriction on the information currently contained in the National Practitioner Data Bank. HCQIA, 42 U.S.C. § 11137(b)(3) (1994) (stating that the information "is intended to be used solely with respect to activities in the furtherance of the quality of health care").


288. Id. ¶ 355.999(2); Johnson, supra note 7, at 411. The AMA does not, however, include license revocations in the information that should be purged. Id.

289. See supra Part III.B.2.b.

290. AMA Pol'y Compendium ¶ 355.998. The AMA argues that physicians must be notified when their file is queried and calls for improved notice procedures. AMA Pol'y Compendium ¶¶ 355.995(4), 355.996, 355.997.

291. Id. ¶ 355.995(4).
3. Enforcement Mechanisms

For a physician data bank to incorporate fair information practices, there must be procedures to monitor the data bank’s accuracy and to challenge an entry claimed erroneous.292 This requirement places more responsibility on agencies such as the Department of Health and Human Services (the agency maintaining the data bank) to ensure that the proper information is collected and monitored for accuracy.293

The National Practitioner Data Bank guidelines mandate that physicians be given access to their own records,294 and have established grievance procedures295 for physicians who wish to contest aspects of their record.296 The AMA Policy Compendium seeks to ensure that physicians continue to be able to attach an explanation to their report in the National Practitioner Data Bank,297 and argues that this explanation should travel with a physician’s report whenever it is used.298 In addition, the AMA also proposes allowing physicians an extended time to verify information reported to the National Practitioner Data Bank.299

4. Special Protections for Sensitive Data

As mentioned earlier, fair information practices require that certain enumerated categories receive extra privacy protection.300 The only information at issue in physician data banks that falls into these categories is information concerning a physician’s health or substance abuse history.301 This Note therefore argues that this information should remain confidential.

This Note expands on the fair information practices categorization of information into degrees of sensitivity by further delineating other categories of information deserving more or less privacy protection.302 While not necessarily “sensitive” in the strict use of the term, other types of information nonetheless deserve privacy consideration based on its inability to meet other fair information practices requirements.

This section argues that certain types of information, including court judgments, state medical board licensing and disciplinary decisions, and education, specialties, and awards, will aid consumers in

292. See supra Part III.B.2.c.
294. 45 C.F.R. § 60.11(a)(2) (1996); see Johnson, supra note 7, at 408.
295. 45 C.F.R. § 60.14; see Johnson, supra note 7, at 410-11.
296. 45 C.F.R. § 60.14.
298. Id. ¶ 355.999(5).
300. See supra Part III.B.2.d.
301. See supra text accompanying note 221 (listing the categories of information traditionally considered “sensitive” and deserving of higher privacy protection).
302. Id.
PHYSICIAN DATA BANKS

Choosing physicians more than they will hurt physicians by their disclosure. Therefore, based on the privacy balancing test, such information should be disclosed. Other types of information, however, such as peer review decisions and malpractice settlements, present a greater threat to physician privacy interests. Therefore, this Note argues that, to remain in accordance with traditional privacy notions and fair information practices, if such information is to be available to the general public, its disclosure should be limited and accompanied by limiting procedures such as end use restrictions.

a. Court Judgments, Criminal Convictions, and State Licensing Denials, Revocations, and Suspensions

Information concerning court judgments, criminal convictions, and medical license denials, revocations, and suspensions is already available to the public from various media. Medical consumers argue that such information is helpful to them in identifying negligent doctors, but that it is often widely dispersed and difficult to obtain, especially when it is needed in a short time period. They argue that because such information is in the public domain, the government cannot rightfully conceal it from the public. As citizens, they have a right to this information. Therefore, this Note argues that because this information is already available, the potential harm to physician privacy interests is minimal. Although there is a valid right of access based on the information's place in the public records, certain privacy protections may still apply. Privacy advocates argue that by compiling the information, a new privacy interest is threatened, and that just

---

303. See Checking up on Your Doctor, supra note 49, at 62 (discussing how licensing and disciplinary reports are available from state medical boards); Wood, supra note 59, at 102 (discussing how court judgments are available through courthouse records).

304. See Margolis, supra note 41, at 25. “[M]ost of the information in the Data Bank is already publicly available, just not easily or consistently available... [B]eing able to access this information from a centralized base will save time, money, and most importantly, lives.” Id. (quoting Laura Wittkin, Executive Director of the National Center for Patients’ Rights, a malpractice victims’ and patients’ rights advocacy group).

305. Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975) (holding that the public has a right to information contained in the public domain). But see Nixon v. Administrator of Gen. Servs., 433 U.S. 425 (1977) (arguing that this right is limited in the interests of national security). But, just because the public has a right to this information does not mean the government should recompile it and provide it in an easily available format.

306. Rep. Ron Wyden argues that, since federal taxes are used to pay for the National Practitioner Data Bank, taxpayers have a right to its information. Margolis, supra note 41, at 24. But see Robert E. Oshel et al., The National Practitioner Data Bank: The First 4 Years, Pub. Health Rep., July-Aug. 1995, at 383, 384 (“Although taxpayer funds covered development and startup costs, the Data Bank currently is funded entirely by user fees.”); NPDB 1996 Annual Report, supra note 256, at 4 (“As mandated by law, all Data Bank costs are recovered from user fees; no taxpayer funds are used to operate the Data Bank. The Data Bank fee structure is designed to ensure that the Data Bank is self-supporting.”).

307. See supra Part III.A.3.
because information is public does not mean the public has an absolute right of access to it in any form. Certain restrictions such as timeliness, accuracy, and relevance may still apply. So long as there are safeguards in place to ensure the information’s accuracy, relevance, and timeliness, disclosure helps more than it harms, and this information should be accessible to help medical consumers choose physicians.

b. Education, Specialties, and Expertise

At first glance, information about a physician’s education, specialties, and expertise, which is widely available through a variety of sources including the American Medical Association’s Web site, seems relevant to consumers’ interests and innocuous to physician privacy interests. Even this information, however, has been challenged by privacy advocates who argue that certain information could be used to target certain doctors or place them in harm’s way. So long as privacy safeguards are in place, this information should be disseminated.

c. Peer Review and Other Similar Information

Whether hospital peer review information should be available to medical consumers to judge their doctors raises the fundamental question whether peer review proceedings can ever serve as evidence of malpractice. At present, most states protect the privacy of hospital peer review proceedings, maintaining that such confidentiality is crucial for effective peer review, and that, because peer review boards

308. United States Dep’t of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989) (“Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.”); see also Beall, supra note 238, at 1256 (discussing Reporters Committee and the proposition that the public availability of one’s criminal past through some sources does not justify its inclusion in a government data bank); Goldstein, supra note 229, at 1213 (“[T]he mere fact that a record has been public historically does not justify continued treatment without first examining the reasons behind the original policy.”).

309. See supra Part III.B.2.a.


311. See, e.g., Angela C. Couch, Note, Wanted: Privacy Protection for Doctors Who Perform Abortions, 4 Am. U.J. Gender & L. 361 (1996) (arguing that publishing certain information may identify doctors who perform abortions and thus endanger them); Mohl, supra note 55, at A1 (reporting the Massachusetts Legislature’s fears that the online data bank could be used by terrorists to target doctors).

312. Jonathon P. Tomes, Healthcare Privacy & Confidentiality 159-60 (1994). In addition, many states have enacted laws to preserve the confidentiality of health care proceedings. See supra notes 107-08 and accompanying text.
PHYSICIAN DATA BANKS

are not courts of law, to publish such information as evidence of negligence would violate physicians' due process rights.313 This traditional treatment of peer review information recognizes the importance of confidentiality in ensuring the integrity of the peer review process.314 Therefore, such information should remain confidential and inaccessible to the general public through a physician data bank.

d. Medical Illnesses and Substance Abuse Problems

Although, if asked, most Americans would say that they would prefer to know if their physician has a medical illness or substance abuse problem,315 the question of whether this information should be disclosed has traditionally been subject to great dispute.316 Although nondisclosure of this information has greater potential to harm patients, information about medical illnesses and substance abuse problems is also arguably more personal and more deserving of privacy protection.317 Records of medical illnesses or substance abuse problems are personal information for which traditionally there has been a higher degree of privacy protection.318 Such information is

313. See supra notes 104-06 and accompanying text.
314. See supra notes 3, 110 and accompanying text.
315. See, e.g., McIntosh, supra note 82, at 317 (discussing how a hypothetical patient would want to know if his surgeon is HIV-positive).
316. See generally Phyllis Coleman & Ronald A. Shellow, Restricting Medical Licenses Based on Illness Is Wrong—Reporting Makes It Worse, 9 J.L. & Health 273 (1994-95) (discussing the debate over restricting the licenses or privileges of physicians with illnesses and whether information about illness-based practice restrictions should be reported and to whom).
317. Id. at 289 ("The threat to confidentiality posed by national data banks increases the potential infringement of the doctor's right to privacy."). Courts, in examining this limited privacy right, have weighed it against the risk of bodily harm to the patient. Id. at 288-89.
318. This is a traditionally "sensitive" category according to fair information practices. See supra note 221 and accompanying text.

An example of the privacy interests at stake with personal information is the debate over whether patients should be apprised of their physician's HIV status. Although most states have statutes to protect HIV positive patients from having hospitals and doctors disclose their HIV status, this privacy right is somewhat weakened when the patient is a physician. See, e.g., Estate of Behringer v. Medical Ctr. at Princeton, 592 A.2d 1251, 1274, 1283 (N.J. 1991) (finding that, as a patient, plaintiff-physician had a right not to have his HIV status disclosed by the hospital and its staff; but that, as a doctor, he did not have a right to keep such information from potential surgical patients); In re Milton S. Hershey Med. Ctr. of the Pa. State Univ., 595 A.2d 1290 (Pa. 1991) (allowing disclosure of physician's HIV status to patients despite the confidentiality provisions of the Confidentiality of HIV-Related Information Act). Most courts, while acknowledging physicians' privacy rights in keeping their HIV status confidential, have nonetheless mandated disclosure on the grounds that such secrecy endangers patients. See, e.g., Fay v. Almaraz, 620 A.2d 327, 339 (Md. 1993) (holding that, as a matter of law, surgeons have a duty to warn patients of an HIV infected condition); Behringer, 592 A.2d at 1283 (same). Most of these decisions, however, are limited to where the plaintiff actually was or had reason to believe he was in physical danger of contracting HIV. Brozoska v. Olson, 668 A.2d 1355, 1367 (Del. 1995); Fay, 620 A.2d at 337. For a patient to be in actual danger, the patient must have undergone or be prepared to undergo treatment by the allegedly dangerous physician. Therefore,
generally protected, and this protection does not completely disappear simply because the subject is a physician. In addition, to a limited extent, federal law protects against dissemination of this information. These are the types of situations in which peer review, as opposed to the public dissemination of information, is most effective. It is preferable to strengthen peer review and consequently encourage physicians to monitor and seek help for one another rather than allow the public access to information that physicians, seeking to preserve their and their profession’s reputation, ultimately may cease to report to peer review boards. Information about physicians’ substance addictions or medical illnesses is not currently contained in the National Practitioner Data Bank. Even if such information were to be collected for peer review purposes, it would be harmful to peer review to disseminate this information.

e. Malpractice Settlements

In most situations malpractice settlement payments should not be included in the information to which the public has access because to do so violates the fair information practices goal of ensuring that only relevant and useful information is disseminated. Although medical consumers desire access to a physician’s history of malpractice payments as a means of identifying negligent doctors, it is unclear

---

319. Behringer, 592 A.2d at 1274 (finding that, even with regard to physicians, hospital has a duty to keep HIV status confidential).

320. Americans With Disabilities Act of 1990, 42 U.S.C. § 12101 (1994). “[E]ven if courts continue to reject privacy claims, illness-based restrictions cannot survive challenges under the ADA.” Coleman & Shellow, supra note 316, at 289. See also Gostin, supra note 121, at 14 (discussing how “[f]ederal law creates strict rules for maintaining the confidentiality of records of patients treated for drug or alcohol dependency at facilities receiving federal assistance” and how government hospitals or private hospitals maintaining records under government contracts are subject to the provisions of the Privacy Act); Schwartz, supra note 125, at 318.

321. Although state and federal statutes such as the HCQIA require that third parties such as peer review committees report actions regarding negligent physicians, the statutes do not mandate that individual physicians report their colleagues to the third-party reporters. While the goal of these statutes is to strengthen peer review, if physicians are fearful of the consequences of self-reporting and monitoring their negligent colleagues, they will not voluntarily engage in the peer review process and such third parties will have less information to report. See supra notes 101-105 and accompanying text.

322. See supra Part III.B.2.a. Settlement payments are different from malpractice payments made to satisfy a court judgment. Court judgments are public records and subject to a different standard of privacy protection. See supra Part IV.B.4.a.

whether *all* malpractice payments are a useful indicator of incompetence.\textsuperscript{324} For example, section 427(d) of the HCQUIA specifically states that "a payment in settlement of a medical malpractice action or claim shall not be construed as creating a presumption that medical malpractice has occurred."\textsuperscript{325} Malpractice information was originally included in the Data Bank merely to *alert* hospital review boards of a potential problem, not to serve as evidence of malpractice.\textsuperscript{326} This wording was included in the Act in recognition of the fact that many physicians prefer to settle "nuisance" suits, rather than waste their time and money taking these frivolous suits to court.\textsuperscript{327}

That more than three-fourths of the reports in the National Practitioner Data Bank are malpractice payment reports\textsuperscript{328} suggests that consumers would be primarily relying on malpractice payments to judge a doctor's competence. Even when the information in the data bank indicates an actual instance of malpractice, however, that information is not necessarily helpful because it may not actually predict whether that physician will commit malpractice again.\textsuperscript{329} According to AMA Trustee Thomas Reardon, M.D., the information is mislead-

\textsuperscript{324} See infra notes 327-37 and accompanying text (discussing the inability of physician malpractice payments to consistently identify incompetent physicians).


\textsuperscript{326} 45 C.F.R. § 60.7(b)(3) (viii) (1996); see Todd, supra note 96, at 377 (quoting from the National Practitioner Data Bank Guidebook (Public Health Service 1994)). Although insurance companies use much of the same information to calculate risk, peer review boards, as required by law, use the National Practitioner Data Bank to obtain information useful for making staff privileges and disciplinary decisions. While insurance companies may use malpractice information to predict future claims, for peer review boards, malpractice payments are not evidence of negligence *per se*, but merely one factor used to assess a physician's competence. See infra notes 327-37 and accompanying text (explaining the difference between using past malpractice history to calculate risk of future suits and the inability of the same information to predict actual incompetence).

\textsuperscript{327} Margolis, supra note 41, at 25 ("It is well known in the medical profession that many malpractice settlements are tiny payments given to ward off nuisance lawsuits by litigious patients who were probably not victims of true malpractice."). A 1990 Harvard University study looked at negligent injuries in New York hospitals and how often those injuries resulted in lawsuits. The study found that only one out of eight patients who were victims of negligent medical injuries actually filed a lawsuit; while at the same time, of those malpractice claims that were filed, less than twenty percent were actually justified. Kong, supra note 28, at 25 (reporting on the study). Attempting to prevent the perception of these frivolous nuisance suits as evidence of physician incompetence, the AMA recommends that only malpractice payments over $30,000 be reported. AMA Pol'y Compendium §§ 355.993(6), 355.999(1) (1996). Presumably, damages of more than $30,000 indicate legitimate claims, while smaller damages under $30,000 are more likely to result from nuisance suits that physicians prefer to pay off rather than argue on the merits.

\textsuperscript{328} At the end of 1994, 82.6 percent of all reports in the National Practitioner Data Bank were malpractice payment reports. Robert E. Oshel et al., *The National Practitioner Data Bank: The First For Years*, Pub. Health Rep., July 1, 1995, at 383.

\textsuperscript{329} See Ryzen, supra note 76, at 429 (discussing whether and how often malpractice claims actually reflect physician incompetence).
ing because, "[v]ery, very good physicians are sued and good physicians who take difficult cases have bad outcomes . . .". Numerous studies have debated the predictability of future medical negligence based on past incidents of malpractice.

For example, Elizabeth Ryzen, in her article, *The National Practitioner Data Bank: Problems and Proposed Reforms*, cites several studies on the predictive value of past malpractice claims. First, she cites a study by the Medical Liability Mutual Insurance Company and the National Association of Insurance Commissioners that found the major factor influencing the amount of malpractice litigation in which a physician was involved was not the physician's competency, but the complexity of the illness. If complexity of the illness influences the amount of malpractice litigation to which a physician is subject, one potential negative result is that physicians will avoid taking patients where the chance of medical "success" is lower.

Doctors and physician advocates claim that numerous reasons, apart from incompetence, cause some doctors to get sued more than others. For example, in the Nov. 9, 1994 Journal of the American Medical Association (JAMA), a study of 8247 Florida doctors concluded that a doctor with even one claim against him was more than two times as likely to be sued again. In the same JAMA issue, however, two Vanderbilt University studies on Florida obstetricians found no difference in the quality of care exhibited by the doctors who had previously been sued for malpractice and those who had not. Such findings indicate that other factors—such as poor bedside manner or poor communication skills—may account for repeated lawsuits. Therefore, while there may be some correlation between past rates of malpractice claims and future claims, a past malpractice claim rate does not necessarily correlate with future acts of negligence.

These and other studies have also indicated, however, that there might be some correlation to actual incompetence where the malpractice damage awards are excessively large or where a single physician has an unusually high number of claims, taking into account the physician's specialty and years of practice. For this reason, some organizations, such as the AMA, advocate disclosure of medical malpractice information that is limited to a certain number of claims or payments.

332. Id. at 430.
333. See Castrone, *supra* note 21, at 3D.
335. Id.
336. Id.
337. Ryzen *supra* note 76, at 432-33.
above a threshold amount. One would hope that by strengthening peer review, physicians who commit egregious or overly numerous acts of malpractice (as represented by a large number of claims or an unusually high payment) would be prohibited from—or at least limited in—practicing medicine. Without proof of such an effectively-functioning peer review system, medical consumers should be allowed to protect themselves by self-screening for such incompetent physicians. Therefore, most malpractice settlement payments are not helpful indicators of malpractice and should not be disclosed, a physician with more than a pre-set number of malpractice claims within a pre-set number of years, or with a settlement payment over $30,000, should be so identified in the Data Bank.

Public depositories that contain medical malpractice settlements create the risk that the public may perceive a settlement payment as evidence of incompetence when, in fact, the number of settlement payments a physician has made may merely indicate how long he has been practicing medicine. Also, publicizing all physician malpractice settlements will unduly prejudice practitioners in certain specialties with higher rates of medical malpractice lawsuits, such as surgeons or obstetricians. Therefore, if malpractice information is to be disseminated, it should be accompanied by information to relativize the data and present it in the proper context. For example, a report on a physician's malpractice payment could be accompanied by the rates of malpractice payments made by physicians practicing in the same location, for the same amount of time, and in the same specialty so that the information recipient would have some basis for judging the information.

When such information is released but does not fill a legitimate public concern, the physician's privacy interest becomes paramount in the privacy balancing test. Thus, by disseminating only limited information in a manner consistent with fair information practices, the

338. AMA Pol'y Compendium ¶ 355.998 (1996). But see Randall R. Bovbjerb and Kenneth R. Petronis, The Relationship Between Physicians’ Malpractice Claims History and Later Claims: Does the Past Predict the Future? JAMA, Nov. 9, 1994, at 1421 (concluding that claims history of all kinds is a reasonable statistical measure, but that certain types of physician claims are better predictors than others).
339. Because rates of malpractice vary by specialty and years of practice, Margolis, supra note 41, at 25, the pre-set amount should be set by a determination of what is egregious based on the standards of the specialty.
340. See supra note 327 (discussing the rationale for a $30,000 threshold).
341. If a typical physician has a thirty-eight percent chance of being sued, see Margolis, supra note 41, at 25, arguably, the risk will increase with each year the physician practices.
342. Johnson, supra note 7, at 408.
343. Surgeons have an over fifty percent chance of being sued. Margolis, supra note 41, at 25.
344. Obstetricians/gynecologists “can expect to be sued at least three times during [their] career.” Id. (quoting Rep. Larry Combest (R-Tex.), an opponent of opening the National Practitioner Data Bank to the public).
model National Practitioner Data Bank would be able to disseminate the information that meets the public goal of obtaining the information necessary to make informed decisions about their health care and protect the information that must remain confidential to ensure physicians’ privacy interests and, consequently, their faith in the National Practitioner Data Bank and the peer review process.

CONCLUSION

Although it is clear that it is in the best interests of medical consumers to have access to information about their physicians in a convenient forum, it is equally clear that physicians have a privacy interest in some information sufficient to afford them certain protections in the manner in which this information is disseminated and used. If the public’s desire for this information is granted without simultaneously respecting physicians’ privacy concerns, physicians will adjust their behavior to protect their privacy interests. As a result, peer review may be compromised, physicians will spend more of their time defending their reputations in lawsuits, and physicians will be less likely to take the more difficult cases for fear of the publicity repercussions should anything go wrong. The end result will be an overall decline in the quality of health care. Limited public access to the National Practitioner Data Bank, with the medical profession playing a part in deciding what information meets patients’ informational needs and health care concerns, provides the public needed information without unduly compromising physician privacy or, ultimately, the overall quality of health care.