University of Dayton Law Review

Volume 12 | Number 2 Article 2

1-1-1987

Medical Privacy and Medical Research: Is Government the Problem or the Solution?

James T. O'Reilly
University of Cincinnati

UNIVERSITY OF DAYTON LAW REVIEW
VOLUME 12 WINTER 1986 NUMBER 2

MEDICAL PRIVACY AND MEDICAL RESEARCH: IS GOVERNMENT THE PROBLEM OR THE SOLUTION?

*James T. O'Reilly**

I. INTRODUCTION

Privacy rights in personal medical files are under increasing strain as government expands its need for the official scrutiny of patient care records. Government is now auditor, researcher, financial partner, or provider of medical care for millions of Americans. As a nation, we offer the appearance of privacy for the individual's medical records, but we lack the coherent quality of privacy protection which must exist before the appearance of confidentiality can become a reality.

Individual privacy rights reflect the good intentions of our legal system toward personal control of personal medical records, but the performance of our federal privacy protection mechanisms has failed to carry out those noble intentions. In the decade since the Watergate scandal and the reform of our information and privacy laws, the performance of these laws has fallen short of our expectations. They have proven to be a poorly conceived set of rigid and evasion-prone legislative solutions. The good intentions of these laws have been lost in the daily operation of the bureaucratic state.

The good intentions which followed the Watergate bugging and surveillance scandal produced no consistent federal reform of the rights of the individual against federal, state, local, and private sector invasions of privacy. The arcane red tape of the Privacy Act of 1974,[1] the proceduralism of the Freedom of Information Act (FOIA) amend-

---

* Lecturer in Law, University of Cincinnati College of Law; corporate practice, Cincinnati, Ohio. B.A., Boston College (1969); J.D., University of Virginia (1974). This paper is derived from an address to the March, 1986, Conference on Privacy and Medical Records Data Sharing, sponsored by the Proprietary Association, in Washington D.C. The views expressed are those of the author alone.

1. Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (1982 & Supp. III 1985)).

ments[2] of the same year, and a number of convoluted disclosure and privacy provisions in health and educational records statutes[3] were enacted to protect a particularly sensitive population—the recipients of medical care. But if the great expectations which followed Watergate[4] are seen in retrospective since 1974, we failed to accomplish what we expected.

This article studies the legislative protection of individual medical records and the impacts of that protection on the medical research needs of today's epidemiology research community. Epidemiology, the study of disease patterns as a means of studying disease causation, is adversely affected when the privacy protection system overprotects documentation needed for research. The happy medium between effective privacy rights and effective medical research may come from a revision of our federal legislative system for medical records handling.

As a first premise, legislation affecting medical records should protect the legitimate interests of the medical patients whose records are sought to be used in the government or the private sector as a basis for conclusions regarding disease causation or treatment. Many important public health decisions involving cancer, new medical technologies, and product safety are generally premised upon data derived from patient medical records.

This article examines the competing interests in privacy and disclosure. It will discuss the context of the information law debate, focusing on the problems which scholars of privacy and information law perceive today. Next, it will offer an analytical framework for use in the disclosure of records under the federal laws governing information and disclosure. Then it will analyze the significance of a few of the cases. Finally, it will address the specific issue of privacy for medical patients

---

2. Act of Nov. 21, 1974, Pub. L. No. 93-502, 88 Stat. 1561 (codified as amended at 5 U.S.C. § 552 (1982 & Supp. III 1985)). The passage of the extensive amendments to the FOIA immediately preceded the adoption of the Privacy Act by the same Congress. *See id.*; 5 U.S.C. § 552a (1982 & Supp. III 1985).

3. *E.g.*, Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 360i(a)(4) (1982); Public Health Service Act, 42 U.S.C. § 241 (1982 & Supp. III 1985).

4. After news coverage of the Watergate scandal led to revelations of the improper use of information by federal officials, much of the legislative debate over the Privacy Act related to the abuses of federal information by federal agencies. *See* SENATE COMM. ON GOV'T OPERATIONS, 94TH CONG., 2D SESS., LEGISLATIVE HISTORY OF PRIVACY ACT 826 (Comm. Print 1976). Senator Edmund Muskie, during the August 20, 1974, markup of the Privacy Act, expressed a "vague kind of fear about central computer records on individual citizens." *Id.* at 55. A chronology of the interest in privacy legislation and the abuses of personal privacy uncovered by the post-Watergate investigations is found in L. SOBEL, WAR ON PRIVACY (1976). The constituency for privacy legislation did, however, predate the Watergate revelations of 1974. UNITED STATES DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973); A. WESTIN, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORDKEEPING AND PRIVACY (1972).

whose adverse drug reactions are increasingly important to public health studies.

II. THE LEGAL CONTEXT

Medical records privacy is best studied within the context of American information law as a whole. That segment of statute-derived administrative law of the last two decades has been founded upon an erroneous but understandable assumption. The privacy and information disclosure issues came to Congress amid great conflict.[5] Congress had assumed that the conflicts could be resolved with omnibus solutions of privacy or information problems detailed in multiple subsections and exceptions within a complex statute to be effective across the wide variety of situations applicable in today's information society. Having begun with that assumption, Congress has not performed the serious task of supervising, funding, explaining, and revising these laws. Congress declared that the battle was won with the passage of legislation but the change Congress sought has occurred only slowly and reluctantly.

As a result, the calculation of a medical record's legal status requires consideration of the vague privacy exemption for government disclosures of government files in the FOIA,[6] a variety of state disclosure laws governing hospital and outpatient records,[7] and a Privacy Act controlling the same issue of disclosures for a smaller set of federal files.[8] Researching the question of medical patient records control has become a journey through an uncertain world of legislative conflicts, traps, and gaps.

---

5. Conflicts over information policy in several United States Supreme Court cases led to the FOIA reform measures. *See generally* SUBCOMMITTEE ON GOV'T INFORMATION AND INDIVIDUAL RIGHTS, HOUSE COMM. ON GOV'T OPERATION & SUBCOMM. ON ADMINISTRATIVE PRACTICE AND PROCEDURE, SENATE COMM. ON THE JUDICIARY, 94TH CONG., 1ST SESS., FREEDOM OF INFORMATION ACT AND AMENDMENTS OF 1974 (P.L. 93-502) (Joint Comm. Print 1975). Personal privacy abuses led to the enactment of the Privacy Act. *See* L. SOBEL, *supra* note 4.

6. 5 U.S.C. § 552(b)(6) (1982).

7. *See, e.g.*, MINN. STAT. ANN. § 144.651 (West Supp. 1987) (patients' bill of rights). *See generally* R. SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 1978-79, at 11 (1979) (compilation of state medical-records privacy statutes).

8. The class of files covered by the Privacy Act of 1974 is limited to those which are in the control of a federal agency, are retrieved by the name or personal identifier of an individual, and are not exempted from coverage by the Act's exceptions. 5 U.S.C. § 552a(a)(1)–(5), (j), (k) (1982); *see also* OFFICE OF MANAGEMENT AND BUDGET, PRIVACY ACT GUIDELINES 1020–23 (1975), *reprinted in* SENATE COMM. ON GOV'T OPERATIONS & SUBCOMM. ON GOV'T INFORMATION AND INDIVIDUAL RIGHTS OF THE HOUSE COMM. ON GOV'T OPERATION, 94TH CONG., 2D SESS., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 S. 3418 (PUBLIC LAW 93-579) (Joint Comm.. Print 1976) (Office of Management and Budget adopts these limitations as its principal interpretation of the Privacy Act). For a discussion of the problems of implementation of the Privacy Act, see Belair, *Agency Implementation of the Freedom of Information Act and the Privacy Act: Impact on the Government's Collection, Maintenance and Dissemination of Personally Identifiable Information*, 1986 JOHN MARSHALL J. PRAC. & PROC. 465 (1977).

A symptom of our nation's disorganized approach to personal privacy is the 1974 enactment of both a federal disclosure law[9] and a federal privacy law affecting the same documents but containing uncoordinated and somewhat conflicting terms.[10] It took Congress a dozen years to recognize that one statute was mandatory, the other discretionary, and that the two had not been designed to complement each other. Agencies began to claim that exceptions to one statute overrode the mandatory aspects of the other, resulting in new and unpredictable exemptions.[11] It was necessary, ultimately, to amend the Privacy Act to correct the error and to accommodate the two conflicting statutes,[12] after each had been litigated at several different courts with a variety of different results.[13]

An important reality is that our system really does not provide much in the way of systemic protection for the individual. Individual citizens must wait until the privacy loss occurs and then fight, after the fact, about how much damage has been done.[14] The system fails to encourage the holders of documents to safeguard their secrecy. The ideal of privacy protections built into our system has been sidetracked because federal agencies are short of resources. The resulting miscommunication has occurred in an environment of less perceptible public attention to individual privacy rights. In recent years privacy concerns have not stirred enough political interest to motivate the passage of serious legislative revisions to the Privacy Act.[15] The year 1984 stirred

---

9. *See supra* notes 1–2.

10. *Compare* Greentree v. United States Customs Serv., 674 F.2d 74 (D.C. Cir. 1982) (holding that material exempted under the Privacy Act is not per se unavailable under FOIA) *with* Painter v. FBI, 615 F.2d 689 (5th Cir. 1980) (holding that material exempted under the Privacy Act is unavailable under FOIA). *See also* Note, *Is the Privacy Act an Exemption 3 Statute and Whose Statute Is It Any Way?*, 52 FORDHAM L. REV. 1334 (1984); Note, *Privacy Act Exemption (j)(2) Does Not Specifically Preclude Disclosure of Information Within Meaning of Exemption (3) of the Freedom of Information Act*—Greentree v. United States Customs Service, *674 F.2d 74 (D.C. Cir. 1982)*, 56 TEMP. L.Q. 127 (1983).

11. *See supra* note 10.

12. Central Intelligence Agency Information Act, Pub. L. No. 98-477, 98 Stat. 2209, 2211–12 (1984) (codified as amended at 5 U.S.C. § 552a(q)(2) (Supp. III 1985)).

13. *See supra* note 10.

14. 5 U.S.C. § 552a(g) (1982) (civil remedies for violation of Privacy Act). Damages may only be obtained when the violation of the Privacy Act is intention or willful. *Id.* § 552a(g)(4). *See also infra* note 25 and accompanying text for a discussion of state remedies applicable to private sector abuses of information.

15. The Privacy Protection Study Commission made detailed recommendations for alteration of the Privacy Act to expand its protection of individuals. *See* PRIVACY PROTECTION STUDY COMM., PERSONAL PRIVACY IN AN INFORMATION SOCIETY 497–536 (1977) [hereinafter PPSC]. Bills to implement these recommendations, however, failed to pass. *See, e.g.* H.R. 5646, 95th Cong., 1st Sess. (1977); S. 1928, 96th Cong., 2d Sess. (1980). Nevertheless, some of the Commission's recommendations were adopted voluntarily. *See* Bassett & Moran, *"Breaking Away": Implementing the Privacy Commission's Insurance Recommendations*, 16 FORUM 587 (1981).

some passions because of its connection with the literary treatment of privacy invasion in the book *1984*, but legislative action responds best to crisis, and privacy has been relegated to the back burner of legislative apathy. Relatively little has been accomplished to improve the system's protection of individual privacy.

III. INITIAL REMEDIES

The condition of United States privacy law in its historical patterns can be analogized to the experience of the Marquess of Queensberry, who drafted the landmark rules of pugilistics in 1867 to outlaw bare-knuckles boxing.[16] The idealistic Marquess tried to civilize a rather basic human pattern of conflict. But he discovered that there would be some difficulty in structuring the patterns of individual conduct so that a socially acceptable sport could be derived from the ancient propensity for combat by brute force.

Our current resolution of the conflict of interests surrounding personal privacy law is today's equivalent of the fistfight stage in the evolution of boxing. We talk a lot about more sensitive policies for data handling. Society, however, is unwilling to pay for anything beyond today's haphazard system, which compels one to fight for privacy as a matter of court awarded damages, rather than to have government provide some protections.[17] Our system is irregular, unpredictable, and costly for the citizen who pays the legal bills for the ostensible protection which private litigation offers only after the privacy injury has been inflicted.

We could learn much from the nations which de-emphasize litigation and encourage systemic protection of personal rights. Other national systems seem to be more rational and protective. With the exception of a dispute over a Swedish study of medical care for a group of patients, which when its privacy loss implications were revealed became

16. The Marquess of Queensberry contributed his personal prestige and guidance to the sport and earned fame from the adoption of his more civilized system. J. CUDDON, INTERNATIONAL DICTIONARY OF SPORTS & GAMES 624 (1980); THE OXFORD COMPANION TO WORLD SPORTS & GAMES 111–12 (J. Arlott ed. 1975).

17. Canada has recognized that a social cost of computer efficiency is the easy invasion of personal privacy rights. "In short, privacy could be the victim of efficiency. . . . Now there is the potential of an ominous shift in the delicate balance of power between the individual and the state; a shift to the side of the custodians of these great reservoirs of instantly-retrievable, personal information." ANNUAL REPORT OF THE PRIVACY COMMISSIONER OF CANADA 1984-85, at 3 (1985). Affirmative governmental protection of privacy, as in the Canadian system, requires a more effective oversight of the creation and maintenance of private data banks concerning individuals. The Canadian system, like those in England and Sweden, offers a model which has been discussed but never proposed for serious legislative consideration in the United States, perhaps because of the lack of a political constituency favoring expenditure of government funds to limit the private collection of

a source of great controversy in Sweden,[18] affirmative privacy protection systems in Europe appear to have worked well. There is a more rational approach in the nations which systematically protect medical records and other forms of patient-identified privacy information.[19]

In the current wave of cross-checking computer data files, the census and tax records have already lost some of their secrecy. Data sharing policies will cause the expansion of the familiar statutory phrase, "confidential except for . . . ." A variety of statutory purposes for data sharing will be expanded to meet the agencies' current needs. Examination of public records of small business operators, individual business and professional people, and the like is becoming more common, since disclosures of the files about these classes of personal activity are not covered by the Privacy Act.[20]

IV. ABSENCE OF SYSTEMIC SAFEGUARDS

Who is in charge of privacy protection? The United States has no one to claim the title. We have declined to create a privacy chief, a leader of the privacy field, as other nations have.[21] Our rules have developed not from a central system of information law interpretations but from the judicial construction of rather convoluted statutes. When Congress passed the Privacy Act in haste at the end of its 1974 session, it could not agree on whether to create a privacy coordinator, nor has the idea gained political support since that time in a budget-conscious

---

18. Even in the most centralized privacy systems, there will be an irreducible number of invasions of personal privacy because of the human ability to devise evasions. Sweden's scandal arose from the monitoring of medical records of individuals without their consent. Lelyveld, *Worried Swedes Questioning Wide Reach of Researchers*, N.Y. Times, Mar. 11, 1986, at A1, col. 1.

19. For example, privacy protection is accorded to health care information in the evidentiary privilege context in virtually all jurisdictions. *See* R. SMITH, *supra* note 7, at 10; Annotation, *Physician-Patient Privilege as Extending to Patient's Medical or Hospital Records*, 10 A.L.R. 4TH 552 (1981).

20. 29 C.F.R. § 1910.20(c)(3) (1986) (permitting unions to review the medical records of their members which are held in employer files, without the consent or knowledge of the employees). Access to employee medical records is also provided for in some union contracts.

21. *E.g.*, Lelyveld, *supra* note 18 (describing Sweden's Data Inspection Board which controls the nongovernmental use of data banks in that nation); *see* General Motors Corp. v. Director of the Nat'l Inst. for Occupational Safety & Health, 636 F.2d 163 (6th Cir. 1980), *cert. denied*, 454 U.S. 877 (1981). This case involved a federal agency's response to a union request for a study of worker health. The federal agency requested access to medical records, and the employer polled the workers. Access was denied by the employer to the medical records of those who did not consent to the disclosure. The government overrode that individual decision and forced the employer to disclose all the medical records. Similar results of NIOSH medical records requests occurred in United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3d Cir. 1980); United States v. Lasco Indus., 531 F. Supp. 256 (N.D. Tex. 1981); United States v. Allis-Chalmers Corp., 498 F. Supp. 1027 (E.D. Wisc. 1980); E.I. du Pont de Nemours & Co. v. Finklea, 442 F. Supp. 821 (S.D. W. Va. 1977).

Congress.[22] Our approach to privacy rights has been to build few statutory systems while allowing the civil damages powers of the courts to determine who receives privacy rights and when they are received.

The labor relations field is not a particularly sensitive forum for assessment of how individual interests can be protected. Because of the collective nature of the union bargaining process, relatively few rights of the individual are left alone. In this field as with others, the United States tends to give only lip service to the ideal of personal consent to examination of medical records by other private or governmental reviewers. As part of recent labor relations adjudications and OSHA decisions, a union today has broad rights of access to individuals' medical records, enjoying a legal presumption of access even if employees individually object to such access.[23] A government agency responding to a union's request for studies of worker health can subpoena the health records of employees if the employer has retained such files, and individual workers lack veto power over the disclosure of their records to federal officials.[24]

Why civil damages instead of systemic protections? The suggestion that the United States needs privacy rules and the analogy to the Marquess of Queensberry experience reflects the conflict of adversaries in which information is a weapon. There is a basic human desire for success in the fight with other persons for economic, personal, or political advantage. Personal information is used in fighting for one's economic or civil rights, or in the support or defense of charges that discrimination has occurred. It is used when labor unions, insurance firms, or product marketers are fighting for the additional market share which comes with signing up more clients, or fighting a tough election or sales campaign.

Are damages an effective remedy? We offer the person who has been offended by a privacy invasion a system of statutory rights based on the ability to sue and win damage awards after an improper disclosure has occurred.[25] State law governs, and state tort law (absent statu-

---

22. Privacy authority in a central agency was recommended by the Privacy Protection Study Commission. PPSC, *supra* note 15, at 37. Such a body would issue interpretive rules, monitor federal and nonfederal activities, research privacy issues, and educate government officials regarding privacy. *Id.* By contrast to our inactivity, Sweden's Data Inspection Board has been in place for a dozen years. Lelyveld, *supra* note 18.

23. 29 C.F.R. § 1910.20 (1986); *see also* Louisiana Chemical Ass'n v. Bingham, 550 F. Supp. 1136 (W.D. La. 1982).

24. *See General Motors Corp.*, 636 F.2d at 163. *See also supra* note 23.

25. It is conceivable that one could win a tort action for improper dissemination of personal information compiled in a private data bank. *See* Senogles v. Security Benefit Life Ins. Co., 217 Kan. 438, 536 P.2d 1358 (1975); Annotation, *Exchange Among Insurers of Medical Information Concerning Insured or Applicant for Insurance As Invasion of Privacy*, 98 A.L.R. 3D 561 (1980).

tory modification) is not likely to be effective for the individual vindication of the right to preserve the privacy of health-related information.[26] Our Privacy Act permits civil damage awards but not injunctions against violations.[27]

An example of the consequences of the inconsistent exception-riddled privacy information system is a recent Wyoming federal court case which awarded damages against the Veterans Administration.[28] The nurses at a federal hospital objected when the hospital disclosed their personnel evaluation files to a fellow nurse who requested them because of dismay over the ratings which had been given by hospital management.[29] The requester had a union position but those whose files were disclosed were outraged when disclosure occurred with the concurrence of the Washington headquarters of the agency.[30] Ultimately, after hiring counsel and pursuing the case for an extended period, the nurses won nominal damages.[31] Beyond the Privacy Act, constitutional due process case law allows damages against government agents who violate privacy, if an egregious offense has occurred.[32] But absent a severe case of abuse, it is quite difficult to assert one's desire for privacy against the government's efficiency-based decision to disseminate a file. Our FOIA recognizes no power of the individual to compel the government to withhold a personal file from disclosure by the agency.[33]

V. MEDICAL DATA EMERGING ISSUES

The private sector's use of personal information is expanding into new areas of medical data as health care providers become even more cost conscious and as the identification of better "risks" for the group

---

26. *See supra* note 25.

27. The Privacy Act, where it applies, permits injunctive relief only in two narrow circumstances: (1) to amend records and (2) to order agencies to produce records improperly withheld. 5 U.S.C. § 552a(g)(2)(A), (3)(A) (1982); *see also* Parks v. IRS, 618 F.2d 677 (10th Cir. 1980). Otherwise, money damages are the only available remedy under federal law. 5 U.S.C. § 552a(g)(4) (1982).

28. Andrews v. Veterans Admin., 613 F. Supp. 1404 (D. Wyo. 1985).

29. *Id.* at 1407.

30. *Id.* at 1408.

31. *Id.* at 1416 (plaintiffs awarded $1,000 apiece—the minimum they could receive under the Privacy Act).

32. Birnbaum v. United States, 436 F. Supp. 967, 983–84 (E.D.N.Y. 1977) (a violation of the first and fourteenth amendments for federal agents to open plaintiff's mail without a warrant); *see also* Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971) (allowing action for damages against United States government for violation of fourth amendment).

33. The Privacy Act grants no power for a reverse-disclosure suit by the subject of the file. *See* 5 U.S.C. § 552 (1982). If such review authority exists, it must be found in the Administrative Procedure Act. 5 U.S.C. §§ 701, 706(2)(A) (1982); *see also* Chrysler Corp. v. Brown, 441 U.S. 281 (1979).

health care system becomes an appropriate marketing strategy. Utilization of health services produces bits of data which cumulatively place the individual into analyzable categories. Data builds the customer profile in health care as in other service sales contexts. Sharing of data among collectors is the most efficient means of building the customer profiles. In turn, the more efficient customer profile reduces the cost of selling the service or product.

In the competitive health care market, use of profile data on past health service use by individual applicants for a health maintenance organization, for example, would be invaluable. Data helps to weed out the high-cost members of a group whose service needs would exceed predictable premium income. But relatively few cases exist in which the individual as a potential customer has been able to assert the right *not* to be included in someone else's computerized data base.[34] As the controversies simmer, the competitive significance of the possession of large sets of individual medical records and the undisclosed inclusion of individuals into medical records data files are likely to be a future source of more privacy litigation. Legislated schemes for balancing privacy protection needs against legitimate reasons for sharing files would be easy to draft but difficult to pass through Congress. Until the demands for privacy protection become more forcefully articulated, the prospects for improved systemic protection do not look promising.

Is the image of protectability real or imagined? Consider the hurdles faced by the individual patient who learns that his or her medical file has been released to an undesired recipient. After the release of personal medical data without the individual's consent to a third party who sought access to that data, the individual might sue and possibly might win *some* money from *some* privacy-invading persons—or federal agencies (if they are not exempted from the Privacy Act)[35]—under *some* circumstances, *if* the individual's counsel is very astute and *if* the court is sympathetic. Privacy invasion tort actions are for wealthy plaintiffs; they are not cases to be taken on contingent fee. These cases are not capable of resolution without extensive billable hours since few private sector lawyers are familiar with the intricacies of privacy litigation. Our system, however, offers only the right to sue after the act, not much in the way of affirmative pre-release protection.

Who has the power and incentive to use the remedies for privacy protection? In nations with more structured systems, power is balanced

34. The right not to be on a computer list of another person may be protected in tort but such a case would be relatively novel in the tort theory of most states. A. WESTIN, *supra* note 4.

35. Exemptions remove many files from the purview of the Privacy Act, and several agencies are per se exempted. 5 U.S.C. § 552a(j)–(k) (1982).

by a statutory delineation of rights and responsibilities, modifying the employer-employee or surveyor-subject legal relationship to accommodate the primacy of the individual's rights.[36] The system for disclosure in the United States dictates that those who have information about the individual can use it subject to the rather remote prospect that they could be sued for damages later. Litigation costs inhibit the exercise of those rights. Ours is a highly decentralized approach to the gathering and use of personal information.

VI. CENTRALIZATION

Centralization of privacy authority is not a panacea for privacy rights enforcement, but it makes a great deal of sense for the individual seeking vindication of the right to be left alone. The one effort we made to centralize, placing power in the Office of Management and Budget to interpret the Privacy Act,[37] was a total failure, as Congress reported in a recent study.[38] There have been many considerations of such privacy structures as a permanent commission or an information administration. In 1977–78, the Privacy Protection Study Commission's extensive study and report called for a systemic improvement in our preservation of individual privacy.[39] With rare exceptions, the excellent report has gathered dust ever since its rational and clear arguments for a privacy protection structure were offered nearly a decade ago. The Administrative Conference's 1986 Grunewald Report was the first effort in ten years to address structural change.[40] It addressed the need for a mechanism by which the individual or business could contest the government's decision to override confidentiality and could oppose a disclosure of information under the FOIA.[41]

In multinational discussions of privacy and data flow, other nations

---

36. *See, e.g.*, 111 Can. Stat 3321 (private organizations are likely to be affected by the soon-to-be-enacted provincial privacy legislation). Sweden's programs are among the world's most privacy sensitive. Lelyveld, *supra* note 18.

37. The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, 1909, *reprinted in* 5 U.S.C. § 552a note, at 417 (1982) (Guidelines and Regulations for Maintenance of Privacy and Protection of Records of Individuals). This authority over the Privacy Act was limited to interpretations and guidance, some of which has been clearly rejected by the courts. Zeller v. United States, 467 F. Supp. 487, 497 (D.D.C. 1979); *see also* Metadure Corp. v. United States, 490 F. Supp. 1368, 1373–74 (S.D.N.Y. 1980).

38. OMB's failure as a privacy protection source is chronicled in COMMITTEE ON GOV'T OPERATIONS, WHO CARES ABOUT PRIVACY? OVERSIGHT OF THE PRIVACY ACT OF 1974 BY THE OFFICE OF MANAGEMENT AND BUDGET AND BY THE CONGRESS, H.R. REP. NO. 98-455, 98th Cong., 1st Sess. 22 (1983).

39. PPSC, *supra* note 15, at 37.

40. M. GRUNEWALD, A STUDY OF THE DESIRABILITY AND FEASIBILITY OF ESTABLISHING AN ADMINISTRATIVE TRIBUNAL TO RESOLVE FREEDOM OF INFORMATION AND OTHER PUBLIC ACCESS DISPUTES (1986).

41. *Id.*

with a higher priority for personal privacy deride the complexities and ineffectiveness of the United States system. By comparison to other technologically sophisticated democracies, the privacy protection systems of the United States fall far short. We have a patchwork rather than a mosaic. Ours is not a privacy-driven system, and ours is not a predictable system. Compared with Canada's effective and official dedication to the privacy ideal,[42] our system of privacy protection is—to return to the Queensberry rules of boxing analogy—an amateur fistfight without consistent rules. Because of the relatively scant attention paid to privacy issues in recent congressional enactments, there are no uniform, predictable "Queensberry" rules to move us beyond individual "fistfighting" and into the system of privacy protection.[43]

VII. SIGNIFICANCE OF FEDERAL AUDITABILITY

In the medical research field, data on individual patients is almost always auditable by government officials under one or another program, including the Professional Standards Review programs, Medicare, Medicaid, biomedical research, and other quality and quantity measures administered by the Department of Health and Human Services.[44] Inspection of medical patient records enables the government to account for its health care dollars and to supervise the work of data collection for later submission to the government by potential marketers of drugs or medical products. Audits are familiar and records inspection is easily anticipated. Thus, an audit often takes patient records for examination, but the patient does not often know why, when, and for what purposes the records are being reviewed.

The potential for an audit, however, does not translate into direct control or release of the records by federal agencies. Indeed, the Supreme Court decided in *Forsham v. Harris*[45] that the right of the government to have access to a contractor's medical records data base did not mean that the contractor should be considered to have the same duties of public disclosure as the federal agencies would have.[46] This is

---

42. *See supra* note 36.

43. Congressional enactments in recent years have even eroded aspects of privacy, for instance, by permitting computer matching of tax and other files for the purpose of detecting a debtor's sources of income. Note, *Federal Government Computer Data Sharing and the Threat to Privacy*, 61 U. DET. J. URBAN L. 605 (1984).

44. These audit powers of different programs vary in their need for personal medical information. The FDA's supervision of clinical records of test subjects in drug and medical device testing, for example, includes very careful examination of the records of patients who receive the tested drug or medical device, 21 C.F.R. § 812.145 (1986), while the Health Care Financing Administration audits patient medical records, *id.* § 482.24, and Health Maintenance Organization audits patient records. *Id.* § 417.236.

45. 445 U.S. 169 (1981).

46. *Id.* at 186.

becoming more important as cancer and other chronic health risks are being studied through the use of large scale epidemiology screening of populations likely to have been exposed to potential carcinogens. Their medical experiences may provide the needed clues to the discovery of the causation of cancer or birth defects. Since the Centers for Disease Control (CDC) operates through entities which are partially state and partially federal in nature,[47] disputes about access to state epidemiological records through the federal access laws have been a complex, controversial topic.[48]

VIII. ANALYZING THE MEDICAL PRIVACY LAWS

The proceeding privacy analysis can be applied to four federal laws which have some influence upon privacy of medical research subjects. The four primary statutory influences on data sharing are contained in the Privacy Act,[49] the FOIA,[50] the Federal, Food, Drug, and Cosmetic Act,[51] and the Public Health Service Act.[52] The analysis we undertake with regard to privacy under these laws must answer four standard questions: Who? What? Why? And when?

We first ask *who* has the information, for no regulation of private collections of data exists in the federal sphere.[53] Only the federal agency data collector is covered, if she is not so fortunate as to be exempted, and not all federal collections meet the criteria for Privacy Act coverage.[54] Medical research records can be considered to be Privacy Act records only in very rare situations in which they have been specially collected, defined, and treated by the collecting agency.[55] Records of patients may be confidential under certain state laws, but their protection and scope vary considerably.[56]

---

47. The state Epidemiology Intelligence Service officers within each state health department are employees of the federal CDC.

48. *Cf.* Kehm v. Procter & Gamble Mfg. Co., 724 F.2d 613, 618–19 (8th Cir. 1983) (epidemiological studies compiled by the Center for Disease Control and various state agencies were key evidence in finding liability against tampon manufacturer).

49. 5 U.S.C. § 552a (1982 & Supp. III 1985).

50. *Id.* § 552.

51. 21 U.S.C. § 360i (1982).

52. 24 U.S.C § 241 (1982 & Supp. III 1985).

53. *See, e.g.*, Freedom of Information Act, 5 U.S.C § 552(a) (1982 & Supp. 1986) ("Each *agency* shall make available to the public information as follows . . . .") (emphasis added).

54. Only a "system of records" which is designated by the agency as being retrieved by the name of the individual is covered. *Id.* §§ 552(a)(5), 552a(b). Therefore, medical records organized by hospital name, clinical investigator, product, investigation number, and other methods are not affected.

55. For example, subjects of an epidemiology study were protected from disclosure under the Privacy Act in a litigated case involving the CDC. Kehm v. Procter & Gamble Mfg. Co., 724 F.2d 613, 618 n.2 (8th Cir. 1983).

56. State protection of medical patient files is discussed in Note, *Privacy Rights in Medical*

Then we ask *what* the information is—the *type* of record—because some records in the federal system are presumed to be private, but most are not.[57] The type of record may be one which is presumed disclosable, like a grant application by a medical school researcher; or legally protectable at the government's option, like a set of drug-efficacy case-report files for patients treated with a new drug; or presumed confidential, like a record of Medicare patient treatments, which enjoys clear statutory protections.[58]

Then we ask *why* it should be considered for confidentiality at all. The strong presumption in favor of disclosure of all federal files found in the FOIA is difficult to overcome.[59] The law presumes a denial of confidentiality. Overriding the presumption in favor of FOIA disclosure involves such an exertion of time and bureaucratic energy that the norm has become one of disclosure. Case-law developments favor disclosure.[60] The affected individual either lobbies for an express exemption from the FOIA or lives with the expectation that his or her data will be released.

Finally, we ask *when* we should look for confidentiality as the appropriate result. The particular law may have included a clear directive not to disclose.[61] That is relatively unusual. Most often, Congress or the state legislature which set up the reporting system requires a balancing test to determine whether disclosure is permissible. The balancing test under federal law turns upon an analysis of what is "clearly" protected.[62] Many disclosures of government files are legitimate; some are unwarranted, but only those medical or personnel files whose release is

---

Records, 13 FORDHAM URB. L.J. 165 (1985). The privilege and protective statutes are listed in R. SMITH, *supra* note 7, at 10.

57. Records presumed to be private, or in other words, records which fall within the coverage of the Privacy Act, are records which contain information about individuals and are maintained by an agency which can retrieve the information by the name of the individual or some other identifying symbol. 5 U.S.C § 552a(a)–(b) (1982).

58. The federal agency has classification power to list a file as a Privacy Act "system of records," as well as power to use discretion toward disclosure once classification has occurred through "routine use" regulations. 5 U.S.C. § 552a(e)(4) (1982). Such agency classifications are readily accepted by the courts. *See, e.g.*, Ely v. Department of Justice, 610 F. Supp. 942 (N.D. Ill. 1985).

59. The FOIA makes an express presumption of disclosure for all federal agency files subject to the Act, 5 U.S.C. § 552(a)(3) (1982), except for those records which fall within nine relatively narrow exemptions. *Id.* § 552(b)(1)–(9).

60. *See generally* 1 J. O'REILLY, FEDERAL INFORMATION DISCLOSURE § 9.07 (1977 & Supp. 1986).

61. Medicare patient files have such a clear direction. 42 U.S.C. § 242m(d) (1982).

62. The FOIA does not allow disclosure of "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6) (1982); *see also* 5 U.S.C.A. § 552 note 134 (West 1977 & Supp. 1986) (collecting cases).

clearly unwarranted are exempted from disclosure under the FOIA.[63]

These basic questions can be applied to an analysis of the four statutory sources of privacy protection, in order to assess the medical subject's rights. Apart from these statutory protections, the option of individual damages litigation against an improper use may exist at state law.[64] But the chances for the individual to win sufficient damages after a high initial outlay of costs are remote, so statutory protection is most important.

A. The Privacy Act

First, the Privacy Act defines the right of federal agencies to set up filing systems on individuals.[65] If a federal agency is covered at all, and not totally exempted like the CIA and FBI,[66] it should comply with the file creation requirements of the Act. The Act is very long and rather tedious; it details the procedural red tape involved in the maintenance of such files, and it allows the individual to ask for copies of his personal records if he jumps through the proper procedural hoops.[67] The appearance of protection of individual rights is greater than the reality. The Privacy Act is not really followed by the agencies as they would, for example, follow the terms of a substantive or enabling statute.

The Privacy Act contains a few provisions which are easily and widely observed, such as the one-time publication of a list of systems and restrictions on social security number use.[68] But as a charter of personal rights, the Act has been a failure. Violation of the Privacy Act's spirit is virtually an everyday occurrence, since the protections that it was meant to provide, such as notification and logging of disclosures, simply have not worked according to the model of the legislation. Violation of the Privacy Act's letter may also be an everyday occurrence, because with so very few enforcement actions and so few reported cases,[69] no one can tell whether its strict wording has been

---

63. *See supra* note 62.

64. State law controls the damage prospects and recoveries for invasions of personal privacy. *See generally* Note, *supra* note 56; Annotation, *supra* note 19.

65. 5 U.S.C. § 552a(e)–(f) (1982).

66. *Id.* § 552(j).

67. *Id.* § 552a(d).

68. A "rider" on the Privacy Act precludes the use of social security numbers. The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, 1909, *reprinted in* 5 U.S.C. § 552a note at 417 (1982) (Disclosure of Social Security Number).

69. There have only been about 100 cases reported under the Privacy Act, most of them trial court decisions on summary judgment, as compared with more than 1,000 reported FOIA decisions, many of them in the appellate courts. OFFICE OF INFORMATION LAW AND POLICY, DEPARTMENT OF JUSTICE, FREEDOM OF INFORMATION CASE LIST (Sept. 1985 ed.) [hereinafter CASE LIST].

matched by strict practice.

Informed observation would suggest that the Privacy Act delivers little of its promised benefits for consumers, medical patients, and others. It offers great promise as a developmental base for refined analysis of individual rights and systemic protections, such as data-base collection protections and better opportunities for the individual to learn in advance of the proposed dissemination of individualized data. As an unfinished base, the Act has become another layer of procedural red tape encumbering administrative agencies' daily work, rather than a total-commitment quality requirement.

B. Freedom of Information Act

The FOIA, in comparison with the Privacy Act, is well known and well understood.[70] It covers huge quantities of documents, not merely those found in certain arrangements of nonexempted file systems which are subject to the narrower Privacy Act. The FOIA is familiar to many newspaper organizations that often use it to disclose to the public controversial information in the hands of the government.[71] Its relatively simple message is that one can ask any federal agency for any document. The public makes written requests, more than 100,000 each year, and the agencies either disclose the documents or claim exemptions.

The FOIA has not been as successful as it might have been. It has clearly been more litigated than anyone expected when the bill was first adopted in 1966.[72] No one is satisfied with the inefficiencies and abuses of the system, including the FOIA's most frequent individual users, federal prisoners. The promise of easy access and rapid decision making in the public interest has generally gone undelivered. It is more predictable than other legislation, but used less often for public goals than for private snooping.[73] Equitable considerations do not limit the ability of the requester, for the agencies and the courts are barred from creating new exceptions to disclosure beyond those provided by the statute itself. None of the users are satisfied with the Act's procedural problems, and its exemptions are difficult to construe.

There is an exemption to the FOIA for personal privacy documents,[74] but there is no personal right to enforce the exemption.[75]

---

70. The FOIA has generated great news media coverage, several books, and more than a hundred published articles. *See id.* at 367–93.

71. The FOIA has been used for obtaining information about spies, drug dealers, assorted criminals, unidentified flying objects, and a host of other controversial issues.

72. S. REP. NO. 813, 89th Cong., 1st Sess. (1965).

73. More than 85% of the FOIA requests received by the Food and Drug Administration, for example, come from agents of business firms seeking useful information about their competitors or about FDA surveillance of their products.

74. 5 U.S.C. § 552(b)(6) (1982).

Every government employee can disclose a requested document to "any person" who seeks its disclosure—but relatively few employees have the authority to officially deny disclosure.[76] At the Food and Drug Administration (FDA), more than 40,000 requests come in each year, most from companies seeking each others' testing or other commercially useful data. At FDA, hundreds of individuals can respond with disclosures and only one, the Associate Commissioner for Public Affairs, can respond with denials.[77] Medical data is most frequently requested from the FDA, and to a lesser extent from the CDC and other agencies of the Department of Health and Human Services.

Because there is no personal right to enforce the personal privacy exemption, an individual who finds that a federal agency has disclosed his personal record under an FOIA request cannot act before or after the disclosure.[78] The individual cannot bring what has been known as "reverse FOIA suits," enjoining disclosure by the agency, to protect a noncommercial interest like personal medical privacy. Relatively few cases have been tried.[79] The better agencies provide for notification before disclosure of the personal information and make a decision only after hearing both sides of the disclosure question, but there is no statutory right to such process.[80] The person whose medical records are released under the FOIA by a federal agency cannot successfully argue that the Federal Torts Claims Act allows recovery, since disclosure is considered to be an intentional tort for which civil damages are not recoverable against the government.[81]

---

75. Though an individual could argue for such a right of self-protection, it is unlikely to be successful. Commercial protections have been possible because of the existence of the Trade Secrets Act, 18 U.S.C. § 1905 (1982), but personal privacy does not receive the same attention. Washington Research Project, Inc. v. HEW, 504 F.2d 238, 244 n.6 (D.C. Cir. 1974); *see also* Florida Medical Ass'n v. HEW, 479 F. Supp. 1291 (M.D. Fla. 1979), *rev'd on other grounds*, 601 F.2d 199 (5th Cir. 1979).

76. A final withholding decision must by made by the agency head or his delegate. 5 U.S.C. § 552(a)(6)(A)(i) (1982).

77. 21 C.F.R. § 20.47 (1986).

78. There is no injunctive remedy available under the FOIA itself, Chrysler Corp v. Brown, 441 U.S. 281, 316–17 (1979), and the disclosure would be intentional, so the negligence-based waiver of sovereign immunity in the Federal Torts Claims Act would not apply. 28 U.S.C. § 2680(h) (1982).

79. *E.g.*, *Washington Research Project*, 504 F.2d at 238, 244 n.6; St. Paul's Benevolent Educ. & Missionary Inst. v. United States, 506 F. Supp. 822, 287 (N.D. Ga. 1980).

80. The FDA might allow personal notice in an individual case, but has no obligation to do so as a matter of law. 2 J. O'REILLY, FOOD AND DRUG ADMINISTRATION § 22.07 (1979 & Supp. 1986). FDA's parent department has an overall rate of releasing 98.9% of all documents requested, which in a calendar year was 101,602 out of 102,279 requests. Burnham, *Assessing Freedom of Information Act*, N.Y. Times, Aug. 29, 1985, at B10, col. 4.

81. 28 U.S.C. §§ 1346(b), 2680 (1980). There would be no recovery in the federal action, and responding to a lawful access request has no counterpart in private nongovernmental activities. Gelley v. Astra Pharmaceutical Prod., Inc., 466 F. Supp. 182 (D. Minn.), *aff'd*, 610 F.2d 558

C. *The Federal Food, Drug, and Cosmetic Act*

The Federal Food, Drug, and Cosmetic Act[82] is a little more explicit about personal and medical information, requiring that drug and medical device patient information be treated with "due regard" for patient rights.[83] Medical device data is subject to a special section of the Act which provides that patient identities may not be required to be disclosed when the FDA audits the activities of a private sector clinic, but the section's exceptions cover broad objectives, such as determining that the device is effective or verifying a test record, which could nullify the anticipated protections.[84] The individual patient whose experience with a drug or device is used in an FDA application is offered protection under FDA regulations,[85] however, and these specifically control the disclosure practices which affect personal data about these patients.

D. *Public Health Service Act*

The Public Health Service Act, governing the roles of the CDC and National Institutes of Health in government-funded disease monitoring and prevention, allows for the disclosure of a wide variety of research data "through publications and other appropriate means."[86] In most cases, the Public Health Service's authority to withhold information comes from the creation of a Privacy Act system of records; in a few cases, such as with Medicare and Medicaid files, special provisions prohibit disclosures.[87] It forms the legal basis for the epidemiological research done by the CDC and National Institute of Occupational Safety and Health (NIOSH), which are segments of the Public Health Service.[88] Disclosure of detailed medical records by these two organizations has been very controversial, since the reports of adverse medical effects by either organization carries important regulatory and public relations consequences for the factories, products, or areas which CDC or NIOSH researchers examine. In *General Motors Corp. v. Director of the National Institute for Occupational Safety & Health*,[89] the

---

(8th Cir. 1979); *see* Note, *Rejecting Absolute Immunity for Federal Officials*, 71 CALIF. L. REV. 1707 (1983).

82. 21 U.S.C. § 360i (1982).

83. *Id.*

84. *Id.* § 360i(a)(4), (b).

85. 21 C.F.R. § 20.111 (1986).

86. 42 U.S.C. § 241 (1982 & Supp. III 1985).

87. *Id.* § 242m(d).

88. Both agencies are currently part of the Public Health Service within the Department of Health and Human Services. OFFICE OF THE FED. REGISTER, NATIONAL ARCHIVES AND RECORDS ADMIN., THE UNITED STATES GOVERNMENT MANUAL 280 (1986–87).

89. 636 F.2d 163 (8th Cir. 1980), *cert. denied*, 454 U.S. 877 (1981).

right of the individual to deny access to his own file was overridden, after the individual preferences had been polled and the files had been acquired by NIOSH.[90] In *Kehm v. Procter & Gamble Manufacturing Co.*,[91] the Eighth Circuit Court of Appeals allowed the use in evidence of a CDC telephone survey which drew conclusions from information concerning former medical patients' symptoms and product causation, with no disclosure of the patient identities and no opportunity for rebuttal of the findings by the CDC's opponents.[92]

IX. THE NATIONAL ACADEMY OF SCIENCES REPORT AND AGENCY ATTITUDES

The sharing of medical data, once collected, can be the basis for multiple examinations of the same disease-causation theory. With sharing, the data can be verified or replicated. The benefits and burdens of data sharing have been capably covered by a National Academy of Sciences (NAS) study issued in 1985.[93] The NAS Committee performed a useful service in suggesting government policy alterations which might provide social scientists and medical professionals with wider access to personal data.[94] But governmental policy, particularly disclosure policy, often clashes with the scientific ideal of academic data sharing which is reflected in the NAS study. Sharing has been inhibited by the FOIA. Prior to that statute's adoption in 1966, governmental policy on data disclosure presumed that data would be withheld until the agency wished to publish it.[95] This well-documented philosophy of tactical nondisclosure might be called the Paul Masson syndrome—"we will disclose nothing before its time." But the selective timing and content of governmental disclosure is no longer legitimate. Federal agencies have been forced by court decisions enforcing the FOIA to release more documents more rapidly in response to more frequent requests. The significance of this historic change in attitudes is that the submitter's reliance in continued confidentiality, which once was exhibited by informal promises of confidentiality by government officials to the private data submitters, has been lost. One not only cannot rely on an informal assurance—one does not get them at all.

Agency managers in the federal system, faced with litigation costs

---

90. *Id.* at 165.

91. 724 F.2d 613 (8th Cir. 1983).

92. *Id.* at 618–19.

93. SUBCOMMITTEE ON SHARING RESEARCH DATA, COMMITTEE ON NATIONAL STATISTICS, SHARING RESEARCH DATA (1985) [hereinafter SHARING RESEARCH DATA].

94. The report approached the issue from statistical, academic, and legal perspectives. *See generally id.* at 3–36.

95. S. REP. NO. 813, 89th Cong., 1st Sess. 2 (1965).

from unsuccessful defenses of FOIA suits, have structured the decisional process about data sharing to take it out of the hands of nonlawyers. A decision to share data with a university epidemiologist is more the responsibility of counsel than of the scientific staff of the agency. Confidentiality promises of the FDA, for example, require a quasi-formal adjudication with detailed legal maneuvering.[96] Furthermore, confidentiality adjudication rights have been contested, sometimes successfully, by persons unhappy with the treatment which FDA gave to their private information.

Secrecy in decision making had been one of the symbols of power possessed by executive agencies. The suddenness of the changing philosophy in the mid-1970's toward less secrecy, combined with the Carter Administration's strong pro-disclosure stance, instituted an FOIA philosophy of "when in doubt, send it out." Case law required an agency which shared a document with one requesting person to disclose it to all subsequent requesters.[97] The pressure to make drafts of new rules available to all sides led to a corresponding limitation on the number of drafts which an agency staff would create and the number of copies which they would circulate.[98] But preservation of internal agency documents as secret did not cause a corresponding sensitivity to the release of nonagency documents.

X. Disclosure Cases in the Courts

A sample of five FOIA cases involving requests for disclosure of arguably personal information illustrates the developments.

In the first case, *Robles v. EPA*,[99] the EPA performed a study of the effect of radon gas on homes which had been built with some potentially radioactive materials taken from a uranium mill site. Though confidentiality had been informally promised,[100] disclosure was ordered by the trial court and affirmed on appeal, with the Fourth Circuit Court of Appeals holding that the equities of the situation, reliance on promises of confidentiality, were overridden by the pro-disclosure approach of the FOIA.[101] Promises of confidentiality for health-related surveys are not enough to overcome the Act's pro-disclosure direction.

The *Robles* court noted that limited disclosures had occurred in

96. 21 C.F.R. § 20.111 (1986); *see* Carson Prod. Co. v. Califano, 594 F.2d 453 (5th Cir. 1979); Zotos Int'l, Inc. v. Kennedy, 460 F. Supp. 268 (D.D.C. 1978).

97. North Dakota v. Andrus, 581 F.2d 177, 180 (8th Cir. 1978).

98. The elimination of ready access to drafts of agency regulations was offset by the lengthier process of review after rules are proposed. *See generally* J. O'Reilly, Administrative Rulemaking ch. 9 (1983 & Supp. 1986).

99. 484 F.2d 843 (4th Cir. 1973).

100. *Id.* at 844.

101. *Id.* at 848.

the past without objection.[102] But now, all the survey results would be released to anyone. Disclosure to all requesters alike may be unfair in terms of consequences to individuals, but it is the FOIA's mandate. The homeowners would be informed whether they were exposed to radon levels above limits, but the same data would be released to anyone, extinguishing any potential for ever selling the homes. The court ordered disclosure of the details even though there had been a confidentiality expectation on the part of the survey participants and even though the individual homeowners would suffer a total loss of marketability of their homes as a result of disclosure.

In *St. Paul's Benevolent Educational & Missionary Institute v. United States,*[103] a church group which was engaged in a public controversy over the effects of infant formula upon child mortality and disease patterns did a survey and accumulated raw data on this subject.[104] The group had a clear advocacy goal for use of that data in a struggle with more economically powerful opponents. The group could leverage its power with governmental assistance, and the government appeared to be sympathetic. The group shared the detailed raw data with the CDC in order to obtain a CDC computer analysis.[105] Then the competing formula manufacturing firms requested that CDC disclose the data which was in CDC's possession to perform their own analysis, before the church group's press release announcing its statistical findings.[106] The CDC made an initial decision and a Washington official, sent as a hearing officer for the appeal, ruled in favor of disclosure to the industry requester.[107]

The church group sued to block disclosure of the raw data. The court dismissed the suit and held that there was no legal right inuring to a nonprofit owner of private data to protect it from a discretionary disclosure by the government.[108]

The National Academy of Sciences' lengthy study, *Sharing Research Data,* covers the *St. Paul's* case in a light most favorable to the researching group.[109] It might have been more just and equitable, perhaps, for the government to have honored the group's expectation of confidentiality. Without confidentiality, for example, the group could not publish its statistics in a peer-reviewed journal and achieve priority

102. *Id.* at 846.
103. 506 F. Supp. 822 (N.D. Ga. 1980).
104. *Id.* at 823–24.
105. *Id.* at 826.
106. *Id.* at 826–27.
107. *Id.* at 827.
108. *Id.* at 828.
109. SHARING RESEARCH DATA, *supra* note 93, at 159 (from a commissioned paper written by J. Cecil and E. Griffin).

of Publication. But in light of FOIA case law, equitable considerations were irrelevant, and the researchers were foolish to expect that the CDC could keep that information confidential. They made a faulty assumption that the government applies one standard of confidentiality to all of its data.

In practice under the FOIA, one must assume that a double standard will be applied when an agency is faced with a request for disclosure of documents which the creator did not yet desire to disseminate at large, because the information is of a draft or evolving policy nature or because premature release would damage some recognizable interest such as the academician's interest in priority of technical publication or patentability of a new invention.[110] The government routinely withholds its own materials as predecisional and therefore premature for disclosure. However, materials of equivalent status, given to the same government agency by private persons, are readily released.[111]

Government applies a double standard to meet its own priorities, and perhaps, the submitting group in *St. Paul's* had received poor legal advice when it shared data with the government as directly as it did. But such dissemination of private data by the government is a natural consequence of having placed "government in a goldfish bowl."

The third case, *National Association of Atomic Veterans, Inc. v. Director, Defense Nuclear Agency*,[112] involved individuals who had been exposed to atmospheric nuclear weapons tests before their discharge from the military. A nonprofit group believed that adverse health effects form exposure remain latent for years before becoming manifest. As a result, the group wanted to solicit former military personnel for joint epidemiological studies and eventual litigation against the government. Names of the individuals were held by the military, ostensibly collected with a promise of confidentiality.[113] The military argued that the group's effort was redundant of existing federal health programs for the same class of persons, so disclosure would not serve a public purpose.

The court held that the fact an individual may have been affected adversely by exposure to radiation, with medical consequences, could be taken into account. But the court ordered disclosure of the lists because inquiries about medical conditions, made after the release of names and addresses, would not in themselves implicate any privacy

110. *Id.* at 178–80.

111. A pre-decisional private document is not exempted unless it fits into one of the special exemption categories. Washington Research Project, Inc. v. HEW, 504 F.2d 238, 244 (D.C. Cir. 1974); *St. Paul's*, 506 F. Supp. at 829.

112. 583 F. Supp. 1483 (D.D.C. 1984).

113. Confidentiality had been promised. *Id.* at 1488 n.6.

concerns, and the public interest in disclosure outweighed medical privacy concerns of the veterans.[114] The court also noted that promises of confidentiality had been made under the Privacy Act and, as noted earlier in this paper, the FOIA disclosure power overrides the Privacy Act withholding authority, so disclosure could be ordered under the FOIA.[115] Despite the confidentiality pledge, therefore, names and addresses were disclosed so that the requester group could contact the 30,000 affected persons.

In the fourth case, *Kurzon v. Department of Health & Human Services,*[116] the appellant, Dr. Kurzon, disputed the government's selective funding of research grants and demanded access to the identities of rejected grant applicants. Dr. Kurzon wanted this information to test his own hypothesis that unorthodox research proposals were generally refused.[117] The district court denied Dr. Kurzon's request, reasoning that the public interest to be served by disclosure was outweighed by the privacy interests of rejected applicants.[118] The court of appeals, believing that rejected grant applicants have very little privacy interest in the disclosure of their identities, reversed the district court's ruling and held that the government had to grant Dr. Kurzon access to the rejected grant applicants' identities.[119] The court believed that the records protected by exemption 6 of the FOIA had to contain personal information consisting of " 'intimate details' of a 'highly personal' nature."[120] The court concluded that the information at issue in this case was simply not intimate enough for exemption 6 protection.

In the fifth case, *United State Department of State v. Washington Post,*[121] the United States Supreme Court decided that citizenship could be "personal" information. The Washington Post wanted information on whether two Iranians who were believed to be in the Iranian capital held United State's citizenship. The FOIA exemption covered personnel, medical, and similar files. The Supreme Court said that virtually any information about an individual which was personal to that individual was enough to meet the "similar" standard but that not all information claimed to be confidential would be protected.[122] This decision broadened the categories which might qualify for protection as similar files but did not change the pro-disclosure presumption of the

114. *Id.* at 1487–88.
115. *Id.* at 1488.
116. 649 F.2d 65 (1st Cir. 1981).
117. *Id.* at 66.
118. *Id.*
119. *Id.* at 68–70.
120. *Id.* at 68. *See supra* note 62.
121. 456 U.S. 595 (1982).
122. *Id.* at 604.

"clearly unwarranted" standard, under which agencies bear a strong burden to hold personnel files as confidential documents.[123]

XI. The Forsham Decision

These five cases illustrate the difficulty of preserving confidentiality for the records of medical research subjects. The landmark Supreme Court case involving medical records of diabetes patients, *Forsham v. Harris*,[124] added a new wrinkle to the law of records disclosure by subcategorizing the possessors of medical records into strict agency/nonagency categories.[125] A lengthy study of diabetes in thousands of patients was conducted under government supervision, and at the government's expense, by a contractor whose work was a direct substitution for a governmental research study by a body such as the National Institutes of Health.[126] Opponents of the study's medical conclusions recognized that the federal sponsor controlled the study, and their FOIA request assumed that the agency controlled the study's records. However, if the records were not released, then the validity of the government's conclusions could not be impeached, since the raw statistical data could not be accessed by researchers who wanted to examine the study's conclusions.

The Supreme Court in *Forsham* held that the government agency responsible for creating and funding the study had lacked physical possession of the diabetes study reports and thus could not be compelled to disclose them even though the study was funded and supervised actively by federal agency personnel.[127] The technical differentiation between "agency record" status and non-record status was imperceptible from outside the agency, but the Supreme Court held it to be legally controlling over the disclosability of the medical information.

XII. Lessons from the FOIA Cases

Forsham was more of a procedural than a policy decision, not helpful to the overall issue of privacy protections for individuals' medical information. For that guidance, it is necessary to distill the dozens of cases dealing with the FOIA and personal privacy.

The first lesson of the FOIA cases dealing with individual privacy is that there can be no legal reliance interest in the exclusive possession of medical or technical data after it is shared with government.[128]

123. *Id.* at 600–01.
124. 445 U.S. 169 (1980).
125. *Id.* at 184–87.
126. *Id.* at 171–74.
127. *Id.* at 186.
128. *Compare* National Ass'n of Atomic Veterans, Inc. v. Director, Defense Nuclear

There will be no blanket assurance of confidentiality. Only totally excluding data from government possession can assure the owner of full recoupment of rights or value in data. Remedies such as damages against the government are quite unlikely. The Supreme Court in *Ruckelshaus v. Monsanto Co.*[129] left open the possibility of Tucker Act[130] relief when commercial technical data is disclosed,[131] but that relief is not likely to be available for personal or medical data. The government has a great deal of discretion in disclosure determinations, and most of the consequences of that discretion are not subject to compensation.[132] Only what government does *not* have in hand, government cannot release.

In the absence of a realistic expectation of confidentiality, the guiding principle should be to watch what people do, not what they say, about trusting government. The creation of special data registries such as the diabetes registry in *Forsham* could be a method of keeping information out of government files and thereby maintain its secrecy. The rise of the confidentiality depositories for aggregate production data during EPA rule making is a reflection of mistrust in the government's confidential handling of valuable commercial data.[133] The sharing of data is often conditioned with safeguards; Congress has been prodded on occasion to adopt stringent nondisclosure requirements for certain agency files containing private sector documents.[134]

Second, once documents are in federal-agency custody, they are subject to the agency's discretion and one cannot expect that a private person will successfully block an agency decision to disclose. The submitter, as patient or as researcher, simply cannot trust government to

---

Agency, 583 F. Supp. 1483 (D.D.C. 1984) (holding that the Defense Nuclear Agency, a government department, had to disclose names of atomic veterans in its possession) *with* Forsham v. Harris, 445 U.S. 169 (1980) (holding that HEW did not have to disclose test data in the possession of an outside contractor).

129. 104 S. Ct. 2862 (1984) (appellee pesticide manufacturer allowed to sue EPA in the United States Claims Court under the Tucker Act to recover for the unconstitutional taking that may result from the use by other pesticide manufacturers of commercially valuable data appellee had to submit to that agency).

130. 28 U.S.C. § 1491 (1982) (allowing claims against the United States based on the constitution and other laws to be brought in the United States Claims Court).

131. *Monsanto*, 104 S. Ct. at 2880–82. Commercial data on pesticide testing was provided to the EPA by an applicant seeking approval of a pesticide. *Id.* at 2871. An argument for extending the Tucker Act to drug information has recently been proposed for clinical data on human test subjects having commercial value. Beers & Zovickian, *Generic Drug Law May Spawn 'Taking' Claims*, Legal Times, Apr. 14, 1986, at 16, col. 1.

132. *Monsanto*, 104 S. Ct. at 2875 (holding that a taking cannot occur when one submits data to a government agency with the knowledge that the information will be disclosed).

133. *Cf.* Pedersen, *Formal Records and Informal Rulemaking*, 85 YALE L.J. 38 (1975) (listing alternative means of collecting data).

134. *See, e.g.*, Drug Price Competition and Patent Term Restoration Act of 1984, 21 U.S.C. § 1431(c)(2) (Supp. III 1985).

withhold documents. Government discretion is ultimately colored by the agency's interests as seen by its lawyers as of the day before trial. Clients must be advised that discretionary decisions are unlikely to be overturned in the courts and that the costs of litigation against a federal agency which seeks a precedential affirmance of its discretion will be prohibitively expensive.

Third, the FOIA cases on privacy are often won by the government. Disclosure to an FOIA requester is not likely to be an actionable source of financial recovery if the agency has followed its normal FOIA procedures.[135] The prospect of a successful action for damages under the Tucker Act is most unlikely absent agency misconduct.[136] In a late 1984 decision, a California fruit-packing firm was awarded millions of dollars in damages resulting from the FDA's issuance of incorrect and unfair publicity about the firm's fruit, which had been packed with cyclamates before that sweetener was banned by the FDA.[137] The firm had to seek congressional passage of a private bill and then endure the litigation costs of a protracted trial in the Claims Court. The decision was later reversed[138] and so the firm still has not collected, fifteen years after the adverse publicity ruined its market in cyclamate-sweetened canned fruits and drove the firm into bankruptcy. The prospect of the medical patient recovering for embarrassment, humiliation, or opprobrium arising out of an FOIA disclosure is illusory. At best, one could argue for constitutional damage recovery, but the odds against recovery are great.[139]

Fourth, disclosure to one requester ends in disclosure to all. There is no selectivity in our system with respect to releases to special classes, except in the rare case of consultants or advisory committee members.[140] The reason why the government is uncooperative toward a

---

135. The Federal Torts Claims Act would not apply because the action was not negligent but was the intentional dissemination of a requested document. 28 U.S.C. § 2680(h) (1982).

136. Orme, *Tucker Act Jurisdiction over Breach of Trust Claims*, 1979 B.Y.U. L. REV. 855, 881–82 (Tucker Act relief is subject to many uncertainties).

137. California Canners & Growers Ass'n v. United States, 7 Cl. Ct. 69 (1984), *rev'd*, 9 Cl. Ct. 774 (1986).

138. *Id.*

139. A federal agency's disclosure is likely to be intentional as to the fact of disclosure and neutral as to intent, so a cause of action for intentional infliction of emotional distress probably would not be available even if the Federal Torts Claims Act were to permit such intentional torts. *See supra* note 135. Disclosure as a result of an FOIA request is presumed lawful. *See* 5 U.S.C. § 552(a)(4)(B) (1982) (burden on agency to show records should be withheld), and would certainly not be the egregious governmental conduct compensable as a "constitutional tort" under Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971), or a deprivation of a constitutional right to privacy without due process actionable under 42 U.S.C § 1983 (1982).

140. Consultants and advisory committee members are not "any person" for purposes of the FOIA's general disclosure provisions which treats all requesters alike. *Cf.* Lead Indus. Ass'n v. Occupational Safety & Health Admin. 610 F.2d 70 (2d Cir. 1979); Wu v.National Endowment

"worthy" researcher may be that agency managers recognize the precedent of release is controlling when others make the identical request.[141] Despite the *bona fides* of one requester, the peril of precedent-making is an important consideration.

Fifth, the terms under which the exemption for personal privacy applies remain fuzzy. The definitions of "clearly unwarranted" and "similar files" are uncertain despite dozens of court cases attempting to clarify the exemption.[142] It is an exemption inherently subjective in scope and unlikely to be amended soon.

Sixth, in this as in other cases, the reality of the bureaucracy overrules the abstraction of the law. The confidentiality of personal data is in the hands of an overworked but dedicated group of disclosure officers. Life in an agency Freedom of Information office presents constant threats of adverse criticism, congressional dismay, and lawsuits if the agency staff chooses to withhold. Mistakes are made and some mistaken releases have privacy consequences. The prospect of private information slipping through the net by error, for instance in the release of a product-application file, is a real one. Some agencies have acted accordingly to reduce their searching and disclosure efforts. Law enforcement agencies won total exemptions from the Privacy Act and have sought comprehensive exemptions from the FOIA out of their concern that convicts could readily use disclosed materials to retrace the actual identities of informants.[143]

Finally, a set of files which meets all Privacy Act requirements and is properly marked and prepared for Privacy Act purposes is more likely than others to be withheld, but no submitter can expect the documents in their entirety to be be subject to Privacy Act protections. Coverage by the Privacy Act is not automatic and not easy to establish for the agency. While an original file marked "John Doe, X Hospital patient" rests quietly, protected under the Privacy Act, a duplicate copy of a medical record may be released from a non-Privacy Act file

---

for Humanities, 460 F.2d 1030 (5th Cir. 1972); Exxon Corp. v. FTC, 466 F. Supp. 1088 (D.D.C. 1978).

141. Disclosure to one private party waives the exempt status of the document upon subsequent request by another party, since the record is no longer "confidential" absent some special disclosure agreement on the first dissemination. North Dakota v. Andrus, 581 F.2d 177 (8th Cir. 1978); *see also* County of Madison v. Department of Justice, 641 F.2d 1036 (1st Cir. 1981).

142. The personal privacy exemption to the FOIA has been litigated in about 320 cases, based upon 1985 statistics for 5 U.S.C. § 552(b)(6) litigation. CASE LIST, *supra* note 69; *see also* 5 U.S.C.A. § 552 note, at 134 (West 1977 & Supp. 1986).

143. Proposals for reform of the FOIA would limit the use of the FOIA by convicted offenders, severely restricting their frequent use of the Act for inspection of law enforcement files. *The Freedom of Information Reform Act: Hearings on S. 774 Before a Subcomm. of the House Comm. on Gov't Operations*, 98th Cong., 2d Sess. 10 (1985); *see also* 5 U.S.C. § 552a(j)(2) (1982) (categorically exempting law enforcement agencies from the Privacy Act).

marked "X Hospital Audit."[144] Then, even if the Privacy Act applies, the routine-use policy of that agency may favor disclosure to a particular type of requester.[145] Routine uses are dislosures made without notice to the file subject.[146]

XIII. Impacts on Medical Research Records

The FOIA and the Privacy Act do impinge on an agency's ability to disclose personal information, but they do not deliver converse reassurance to the medical patient that his or her rights will be sufficiently protected. The good news is that data can be protected when conditions permit and a Privacy Act system applies or has not been avoided through a routine-use regulation. The bad news is that the subject of the medical research may not be sure whether his or her information is secret in the hands of an impersonal bureaucratic health care machine.

Selective disclosure authority may be highly desirable. Epidemiology, the study of disease patterns and causes, would benefit from even greater sharing of limited segments of data taken by a neutral, privacy-sensitive screener from a review of patient records. Government has a large investment in the progress of epidemiology and feels strong incentives to increase its effectiveness as a disease-fighting weapon of medical research.[147] The disclosure of personal medical information to other epidemiologists who are studying the same rare disease condition could have a net societal benefit, because their cumulative efforts to understand disease causation could hasten the achievement of a cure for the disease. The Privacy Act may act as a deterrent to participation for some studies. Certainly the FOIA's pro-disclosure propensities have caused some hesitancy among some of the potential sources of medical data. Fixing the problem with a reasonable statutory amendment for epidemiological research may be the optimal solution.

XIV. Impacts on Disease and Injury Data Gathering

The impact of the privacy and information system on communications about personal illness, such as adverse drug reactions, merits fur-

144. A file is not covered by the Privacy Act unless the file is "assigned to the individual" and retrieved from a "system of records" by the personal identifier of the individual, such as a name or social security number. 5 U.S.C. § 552a(a)(5) (1982).

145. *Id.* § 552a(a)(7), (b)(3).

146. *Id.* § 552a(b)(3). Courts have been supportive of a broad exclusion of such records from notification to the individual, permitting agencies to use the broad "routine-use" exemption to avoid notification. Ely v. Department of Justice, 610 F. Supp. 942 (N.D. Ill. 1985).

147. For example, the CDC, the EPA, and the FDA support epidemiological data-gathering, and with more attention to chronic illnesses, the government has considered "more frequent and wider studies" of exposures and risks to toxic materials. Toxic Substances Strategy Comm., Council on Envtl. Quality, Toxic Chemicals and Public Protection 75 (1980).

ther research by social scientists in the fields of organizational behavior, sociology, and epidemiology. While the system of processing individual data into epidemiology data bases appears to proceed routinely, the conditions underlying this communication may not be optimal for the individual who has been the subject of the shared records.

The adverse drug-reaction reports flowing into the FDA from physicians and hospitals, and from the FDA's own surveillance, are computer-recorded and microfilmed; the original copies are promptly destroyed. The FDA makes it nearly impossible for the identities of the patients to be released, first by computer safeguards within the Office of Epidemiology and Biostatistics, and second by a tough FOIA regulation insisting that identity information will not be disclosed.[148]

Medical records included in these voluntary reports are not the sole source of privacy concerns. The FDA also pays attention to the adverse drug-reaction reports which are filed by the manufacturers of drugs, as required under the 1985 regulations on new drugs and the comparable reports for medical devices.[149] These reports list associations with, not causes of, illnesses, since many of the reports do not reflect a cause-and-effect relationship between the product and the injury.

Cumulatively, the 60,000-plus drug-reaction reports and 20,000-plus device reports allow the FDA to perform rapid examinations of the potential risks of new and existing items and to plot the trends for further study by epidemiologists.[150] A skilled researcher using adverse-reaction data, prescription-volume data from marketing services, and disease-demographic information from the CDC, can propose significant correlations between diseases, responsive drugs' relative effectiveness, and the likelihood of adverse consequences from drug usage.

XV. TORT LAW AND EPIDEMIOLOGY

It is in the pre-discovery and even pre-litigation stages of products-liability litigation that the FOIA is most useful to civil-litigation coun-

148. FDA collection of information about adverse patient drug reactions is explained in 21 C.F.R. § 314.80 (1986) (subsection (h) of section 314.80 prohibits the inclusion of patient identifications in adverse drug reaction reports); *see also* DIVISION OF DRUG & BIOLOGICAL PRODS. EXPERIENCE, CENTER FOR DRUGS & BIOLOGICS, POSTMARKETING REPORTING OF ADVERSE DRUG REACTIONS (1985) [hereinafter GUIDELINE].

149. 21 C.F.R. § 314.80 (1986) (on adverse drug-reaction reports); *id.* § 804.24 (adverse devise-reaction reports).

150. The ability of the FDA to monitor the incoming reports is critical to its approval of new drug and medical-device products. Limited test populations of between 200 and 1,000 patients may participate in the research use of new drugs and medical devices, but millions are exposed after marketing. The FDA regulations are intended to screen out expected and normal reactions from unexpected ones; FDA can then remove an unexpectedly dangerous drug from the market. See GUIDELINE, *supra* note 148.

sel, and it is in this phase that the loss of an expectation of confidentiality becomes significant. The sharing of privately compiled data with the government exposes the data to FOIA disclosure requirements and the problems that inhere in this process. Typically, the goal of an academic researcher is to find a statistically valid correlation between disease occurrence and personal exposures to potentially causative factors. The reward for the academic epidemiologist is priority of publication, being first to discern and report a probable relationship. The publication process itself adds to the pressure for secrecy about the data findings.

Epidemiologists might continue their cooperative data sharing with the government, notwithstanding government disclosure trends, simply to obtain more grant funding or to cooperate with government-paid researchers in the same collaborative projects, if they care to do so. But the flow of adverse reaction data is limited by the realization that government disclosure may be required, with adverse consequences for our information system. The frustration for epidemiologists is that an imbalance exists—too much data can be obtained by those plaintiffs in liability cases with no incentive to pursue societal health goals, while too little is available to medical research academicians because of the concern that openness allows too much damage to the product or the agency program which is affected by the data. The irony is that adverse-experience reports can often be accessed in products-liability suits when the challengers demand full raw-data files from the company which has possession of those files.[151] The challenger has the legal power which the neutral or non-governmental researcher lacks to access the manufacturer's complete factual record on a suspected problem drug.

The government's ambivalence toward disclosure of the patient adverse-reaction reports may be a source of frustration to academic researchers. Release to one person is release to all, ending the expectation of being first to reveal a statistical finding. Private data bases are on a different basis than federal data bases; they need not disclose and they may face some privacy disputes with hospitals or state officials, perhaps, if they disclose too much data too freely. An as-yet-undetermined influence is federal prosecution of regulated firms for being too slow publicly to report problems experienced with products. Faster disclosure of adverse reactions by the makers of the products, upon transmission of the report to a manufacturer from an academic researcher, may be an inevitable cost for the academician as an indirect result of gov-

151. FED. R. CIV. P. 26(b); Note, *The Liability of Pharmaceutical Manufacturers for Unforeseen Adverse Drug Reaction*, 48 FORDHAM L. REV. 735 (1980).

ernment's time pressures upon the manufacturers.[152]

The tort system is not merely a casual presence on the scene; its influence on the process of collecting disease-causation data is so great that it cannot go unnoticed. Plaintiffs may need medical epidemiology data in order to lay the foundation for expert testimony on complex issues of causation. For example, conclusions of an expert concerning causation may involve heated debates over the validity and study design of an epidemiologic study.

It is natural, then, that tort law and scientific rationales for data sharing will collide over the question of access to medical records in drug therapy for disease conditions. The epidemiologist may feel frustrated that in an open and information-oriented society so many governmental, institutional, and litigation incentives have combined to make useful data even less accessible for use than it has been in the past. The science of epidemiology may be retarded in its growth by this combination of constraints against the sharing of data, as well as the constraints put upon future validation or reexamination of the analyses of raw data by later scientists.[153]

Yet another frustration for the medical researcher seeking medical patient files may be with government agencies which have had such great control over information. If agency managers ever decided to maneuver figures to serve a short-term political or bureaucratic goal, their choice not to share the raw data would be legally difficult to challenge. Under case law, the walls of secrecy protecting motives and intentions of federal officials would probably preclude an effective challenge by any private party.[154] The impeachment of an improper motive of a federal official is already quite difficult; where epidemiology is involved, the burden may become insurmountable.

XVI. REMEDIES

Citizens concerned with the privacy of their medical records and epidemiologists seeking portions of those records for use in medical research are not likely to get any relief from Congress for the frustrations discussed in this paper. The specific statutes which need to be amended

---

152. Loss of the novelty of a finding that a product is associated with a physiological effect may be a loss to the priority of publication of the scientist. Such priority of publication is an important rationale used in denying other researchers access to one's compilation of data. *See* SHARING RESEARCH DATA, *supra* note 93, at 136. With the advent of deadlines for filing of data with the FDA and with public access to that data, either the FDA's press office or a competitor which observes adverse reaction rates may announce the possible correlation well before the academician can obtain scientific peer review and publication for epidemiologic findings.

153. A review of the legal status of epidemiologic data is found in Black & Lilienfeld, *Epidemiologic Proof in Toxic Tort Litigation*, 52 FORDHAM L. REV. 732 (1984).

154. Morgan v. United States, 304 U.S. 1, 18 (1938).

are the FOIA and the Privacy Act, and these statutes are nearly impossible to amend because of political constraints.[155] Legislative reform of the medical data process depends on whether the patience, the money, the lobbying talent, and the coalition for political support are available. If not, a special amendment to the Public Health Service Act might be an appropriate alternative solution.[156]

There are some remedies short of statutory changes which may be helpful. Interested users of medical data who wish to gather data outside of government may read *Forsham*[157] and work with agencies to set up depositories. If one wants access to the existing data of federal agencies, negotiations can be attempted, and the agencies have considerable leeway to find exceptions to the privacy protections of the several statutes.[158] In some cases, vigorous efforts may lead the government's lawyers to compromise allowing for access as was done with some of the Reyes Syndrome material needed for products-liability litigation over aspirin.[159] Persistence is likely to be persuasive with the government's lawyers, who will make the final strategic decisions on which cases of statistical secrecy to defend.

XVII. CONCLUSIONS

Ultimately, those interested in medical research and those concerned about medical patient privacy must work out a statutory program of protections. Accommodation to today's confusion is not enough. A better assurance to the individual medical patient about the privacy of the contents of identifiable individual information is necessary. A more balanced, better-coordinated legislative package for epidemiologic research use of personal medical records will be necessary. The constituency for changes to privacy law has yet to be formed, but as more attention is paid to institutional sharing of medical records with government agencies, more attention to privacy concerns is likely

155. Political resistance to reform of the FOIA has made amendments unsuccessful in each session of Congress since 1979, but the effort has continued. *See* S. 774, 98th Cong., 1st Sess. (1985).

156. An amendment to 42 U.S.C. § 241 (1982) might be most appropriate, defining the scope of protection to be accorded when personal medical records are inspected or abstracted by the federal agencies such as the CDC.

157. 445 U.S. at 169. *See supra* notes 124–27 and accompanying text.

158. An agency need not cite an exemption since the FOIA's exemptions are permissive. 5 U.S.C. § 552(b) (1982); *see* Chrysler Corp. v. Brown, 441 U.S. 281 (1979). *See generally* 1 J. O'REILLY, FEDERAL INFORMATION DISCLOSURE § 9.05 (1982 & Supp. 1986).

159. With the government's consent, a limited access compromise permitting epidemiologic researchers representing private manufacturers of aspirin were allowed to examine the data underlying the federal CDC study of aspirin and the state studies of the much-debated linkage of aspirin and Reyes Syndrome. Bunch v. Dow Chemical Co., No. 6442 (Md. Cir. Ct., Montgomery County, Dec. 16, 1985).

to be heard.

Looking back at the challenges faced by the Marquess of Queensberry in the nineteenth century, we can only conclude that our society needs some source of respectable regulatory imposition of rules about privacy. We could benefit from a more civilized form of individual competition over privacy issues. In the longer term, a centrally coordinated federal privacy administrator appears most appropriate. The Marquess proved that it is not enough to invent a better set of rules but that reformers must also develop the stamina, footwork, and fortitude to successfully develop a coherent and workable medical data sharing system for the twenty-first century.