No. 02-20792

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

THE ASSOCIATION OF AMERICAN PHYSICIANS & SURGEONS, INC., CONGRESSMAN RON PAUL, M.D., DAWN RICHARDSON, REBECCA REX AND DARRELL MCCORMICK,

Plaintiff-Appellants,

v.

UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES AND TOMMY G. THOMPSON, SECRETARY, DEPARTMENT OF HEALTH & HUMAN SERVICES,

Defendant-Appellee

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HONORABLE SIM LAKE

BRIEF FOR APPELLEES

ROBERT D. MCCALLUM, JR.
Assistant Attorney General

MICHAEL B. SHELBY
United States Attorney

MARK B. STERN
(202) 514-5089
CHARLES W. SCARBOROUGH
(202) 514-1927
SAMBHAV N. SANKAR
(202) 514-0236
Attorneys, Appellate Staff
Civil Division, Room 9108
Department of Justice
601 "D" Street, N.W.
Washington, D.C. 20530

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 02-20792

THE ASSOCIATION OF AMERICAN PHYSICIANS & SURGEONS, INC., CONGRESSMAN RON PAUL, M.D., DAWN RICHARDSON, REBECCA REX AND DARRELL MCCORMICK,

Plaintiff-Appellants,

v.

UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES AND TOMMY G. THOMPSON, SECRETARY, DEPARTMENT OF HEALTH & HUMAN SERVICES,

Defendant-Appellee

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

STATEMENT OF JURISDICTION

Plaintiffs invoked the jurisdiction of the district court under 28 U.S.C. §§ 1331 and 1337. The district court entered its order of dismissal on June 14, 2002, and plaintiffs filed a timely notice of appeal on July 11, 2002. See Fed. R. App. P. 4(a). This Court has jurisdiction pursuant to 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

The Health Insurance Portability and Accountability Act ("HIPAA"), enacted by Congress in 1996, requires the Department of Health and Human Services ("HHS") to promulgate standards for the privacy of individually identifiable health information. The questions presented in this appeal are:

1. Whether the plaintiffs' First and Fourth Amendment claims are barred on standing and ripeness grounds.
2. Whether the plaintiffs have standing to pursue their Tenth Amendment claim or, alternatively, whether that claim fails as a matter of law.
3. Whether the privacy regulations promulgated by HHS under HIPAA comply with the Regulatory Flexibility Act.

STATEMENT OF THE CASE

Plaintiffs challenge the lawfulness of regulations promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996). In their complaint, plaintiffs asserted that the regulations contained in 45 C.F.R. Parts 160 and 164, generally known as the "Privacy Rule," violate the First, Fourth, and Tenth Amendments of the United States Constitution. Plaintiffs also raised various statutory challenges to the Privacy Rule, contending that the regulations: 1) exceeded the scope of authority granted by HIPAA, 2) violated the Paperwork Reduction Act ("PRA"), 44 U.S.C. § 3501 et seq., and 3) violated the Regulatory Flexibility Act ("RFA"). 5 U.S.C. § 601 et seq.

The district court dismissed each of the claims in plaintiffs' complaint, finding that the plaintiffs lacked standing to assert their constitutional claims, that the First and Fourth Amendment claims were unripe, and that none of

plaintiffs' statutory claims stated a claim upon which relief could be granted. Plaintiffs have appealed the dismissal of their constitutional claims and their claim that HHS violated the RFA, but have not appealed the dismissal of their other statutory claims.

STATEMENT OF FACTS

A. Statutory Framework

Congress enacted HIPAA on August 21, 1996. Subtitle F of Title II, entitled "Administrative Simplification," which is at issue in this case, seeks to improve health care systems nationwide by "encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information." 42 U.S.C. § 1320d note.[1/]

[1/] Subtitle F of Title II of HIPAA consists of sections 261 through 264. Section 262 amends Title XI of the Social Security Act, 42 U.S.C. § 1301 et seq., to add a Part C, entitled "Administrative Simplification," with sections 1171-1179. Those sections are codified at 42 U.S.C. § 1320d through § 1320d-8. Section 261 is found in the United States Code as a note to 42 U.S.C. § 1320d. Section 264 is found as a note to 42 U.S.C. § 1320d-2. Section 263 amends the Public Health Service Act, at 42 U.S.C. § 242k(k). For simplicity, defendants' citations will refer to HIPAA by its United States Code citation.

To accomplish this goal, Congress required HHS to adopt uniform standards "to enable health information to be exchanged electronically." Id. § 1320d-2(a)(1). Congress directed the Secretary to adopt standards for unique identifiers to identify individuals, employers, health care plans, and health care providers across the nation, id. § 1320d-2(b)(1), and standards for, among other things, transactions and data elements relating to health information, id. § 1320d-2(a),(c) & (f), the security of that information, id. § 1320d-2(d), and verification of electronic signatures. Id. § 1320d-2(e).

Congress also recognized that the unified medical information scheme it had established posed risks to the privacy of confidential patient information. Accordingly, it included within Subtitle F a provision — section 264 – that directed HHS to submit to Congress "detailed recommendations on standards with respect to the privacy of individually identifiable health information" within one year of HIPAA's enactment. 42 U.S.C. § 1320d-2 note paragraph (a). Congress also provided that if it did not enact legislation covering these matters within three years, HHS was obligated to promulgate final regulations "containing" such standards. Specifically, section 264(c)(1) of HIPAA provides:

> If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by [August 21, 1999], the Secretary of Health and Human Services shall promulgate

> final regulations containing such standards not later than [February 21, 2000]. Such regulations shall address at least the subjects described in subsection (b).

Id. § 1320d-2 note paragraph (c)(1).

Section 264(c)(2) of HIPAA provides that the privacy regulations promulgated by HHS "shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation." 42 U.S.C. § 1320d-2 note paragraph (c)(2).

B. The Rulemaking Process

As required by Congress, HHS submitted recommendations for protecting the privacy of individually identifiable health information on September 11, 1997. Congress did not act by August 21, 1999, and under Section 264(c)(1), the Secretary then became obligated to promulgate privacy regulations. The Secretary issued a notice of proposed rulemaking shortly afterward, and the sixty-day comment period closed on January 3, 2000, 64 Fed. Reg. 59918 (Nov. 3, 1999), and was then extended to February 17, 2000. 64 Fed. Reg. 69981 (Dec. 15, 1999). HHS received approximately 52,000 public comments during that time period. On December 28, 2000, the Secretary published the final Privacy Rule, effective February 26, 2001. Covered entities were given two years to comply with the Privacy Rule, except for small health plans, which were given three years to achieve compliance.

65 Fed. Reg. 82462 (Dec. 28, 2000).[1/]

On February 13, 2001, HHS submitted the final rule to Congress pursuant to the Small Business Regulatory Enforcement Fairness Act ("SBREFA"). See 5 U.S.C. § 801(a)(1)(A). Because that statute requires that Congress have a full sixty days in which to disapprove the rule, should it so choose, HHS amended the effective date of the Privacy Rule to April 14, 2001. The compliance dates were likewise extended to April 14, 2004 for small health plans, and April 14, 2003 for other covered entities. 66 Fed. Reg. 12434 (Feb. 26, 2001). On February 28, 2001, the Secretary invited the public to submit additional comments on the Privacy Rule for a thirty-day period. 66 Fed. Reg. 12738 (Feb. 28, 2001). The effective dates were not further extended as a result of the additional comment period. HHS recently published final modifications to the Privacy Rule. 67 Fed. Reg. 53182 (August 14, 2002).

C. The Privacy Rule

[2/] This scheme reflects the delays required by 42 U.S.C. § 1320d-4(b)(1).

The Privacy Rule protects the confidentiality of individually identifiable health information. It establishes a set of definitions, state law preemption requirements, compliance and enforcement requirements, and specific privacy protection standards with which covered entities must comply.[1/] These standards relate to the use and disclosure of "protected health information," the rights of individuals with respect to their own health information, and the procedures for exercising those rights. See generally 45 C.F.R. Parts 160 and 164.

The phrase "protected health information" is defined generally by the regulations as—

> [I]ndividually identifiable health information . . . that is (i) Transmitted by electronic media; (ii) Maintained in any medium described in the definition of *electronic media* at § 162.103 of this subchapter; or (iii) Transmitted or maintained in any other form or medium.

45 C.F.R. § 164.501. The term "individually identifiable health information" is in turn defined in 5 U.S.C. § 1320d(6) as:

> any information, including demographic information collected from an individual, that–
> (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
> (B) relates to the past, present, or future physical or

[3/] "Covered entity" means "a health plan," a "health care clearinghouse," or a "health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." 45 C.F.R. § 160.103.

> mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and–
>
> (i) identifies the individual; or
>
> (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

These definitions cover virtually any patient information which might conceivably be considered private. In general, a covered entity may not use or disclose such information except as required or permitted under the regulations. 45 C.F.R. § 164.502. For some uses and disclosures, a covered entity must obtain a patient's written authorization. Id. § 164.508.[1/] Certain other uses and disclosures are permitted (but not required) without authorization. Id. §§ 164.502, 164.510, 164.512, 164.514. These permissive disclosures allow covered entities to release protected health information in order to comply with other laws, such as those authorizing the reporting of child abuse, id. § 164.512(a); id. § 164.512(b)(ii), and to comply with authorized law enforcement and oversight requests. Id. § 164.512(d); § 164.512(f); see generally id.

[4/] The requirement that certain providers obtain consent prior to the use of a patient's health information for certain purposes was dropped by the August 14, 2002 modifications of the Privacy Rule. See generally 67 Fed. Reg. 53182 et seq.

Provisions for compliance and enforcement of the Privacy Rule are set forth in Subpart C of the Privacy Rule's General Administrative Requirements. Id. § 160.300 et seq. These enforcement provisions include the only part of the Privacy Rule that affirmatively mandates disclosure of a patient's private information by covered entities to anyone other than the individual or his or her personal representative. Under the Rule, a covered entity must cooperate with HHS "if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity to determine whether it is complying with [the Privacy Rule]." 45 C.F.R. § 160.310(b). As part of that cooperation, a covered entity must allow access by the Secretary to its "facilities, books, records, accounts, and other sources of information, including protected health information," during normal business hours,[5] but only if that information is "pertinent to ascertaining compliance with the applicable requirements." Id. § 160.310(c)(1) (emphasis added). The Secretary is explicitly forbidden to disclose any protected health information he obtains "except if necessary for ascertaining or enforcing compliance" or if otherwise required by law. Id. § 160.310(c)(3). In other words, if the Secretary decides to investigate a covered entity to determine whether it

[5] Under extreme circumstances (such as to prevent imminent destruction of documents), the Secretary may demand access without prior notice. Id. § 160.310(c).

is implementing HIPAA's privacy guarantees, the Secretary is entitled to examine facilities, books, records and accounts that may contain protected health information, but cannot disclose that information for any purpose other than enforcement, except where other law requires such disclosure.

D. Proceedings Below

Plaintiffs are an association of physicians, the Association of American Physicians and Surgeons, Inc. (AAPS), and individual physicians and patients who object to compliance with the Privacy Rule on a variety of different grounds. On August 30, 2001, plaintiffs challenged the lawfulness of the Privacy Rule as a violation of their rights under the First, Fourth, and Tenth Amendments, and on the grounds that HHS violated various federal statutes, including HIPAA, the Paperwork Reduction Act (PRA), and the Regulatory Flexibility Act (RFA), in promulgating the Rule. In a decision issued on July 17, 2002, the district court dismissed plaintiffs' claims in their entirety. RE4.[1/]

[6/] The district court's decision is published at 2002 WL 1917633, but citations to that decision in this brief are to the the Record Excerpts in this case (e.g., "RE4" references material contained at Tab 4 of the Record Excerpts).

After summarizing the provisions of the Privacy Rule challenged by plaintiffs, the district court dismissed their Fourth Amendment claim on both standing and ripeness grounds. The plaintiffs asserted that they would suffer injury if their health information were accessed without their permission through the provisions of the Privacy Rule. But the district court recognized that "only one provision of the Privacy Rule, 45 C.F.R. § 160.310(c), requires that covered entities provide the government access to protected health information" and that access under this provision was limited to ensuring compliance with the rule. RE4 at 5 n.4. The court thus concluded that "[a] number of unlikely events must occur in order for plaintiffs to sustain an injury." Id. at 5. Among other things, the Secretary of HHS would have to exercise his oversight power to monitor compliance with the Rule, then choose to proceed against a health care entity that held the plaintiffs' health care information, and then request the plaintiffs' information specifically. Id. Given this hypothetical chain of events, the court stated that it was "highly speculative and unlikely that plaintiffs would ever be injured by the Privacy Rule," id. at 5, and therefore held that plaintiffs' pre-enforcement Fourth Amendment claims were "premature and not ripe for judicial review." Id. at 6.[1/]

[7/] To support this result, the court also pointed out that compliance with the Privacy Rule was not required until April 14, 2003, and that "intervening agency action" might make any decision by the court advisory. RE4 at 5. The court further

The district court next dismissed plaintiffs' First Amendment claim for lack of standing. The plaintiffs claimed that the Privacy Rule would have a "chilling effect" on doctor-patient communications. But as the district court observed, the plaintiffs only alleged that "the mere existence of the Rule makes them 'reluctant' to speak freely with their physicians." RE4 at 6. The court found that such allegations "are not an adequate substitute for a claim of specific present harm or a threat of specific future harm." Id. As a result, the court concluded that the plaintiffs had "failed to demonstrate any concrete, particularized, actual, or imminent 'injury in fact' arising from enforcement of the Privacy Rule." Id. at 7 (citations omitted). Moreover, it concluded, "it is unlikely that the plaintiffs' alleged injuries 'can be redressed by a favorable decision' in this case." Id. (citations omitted). Accordingly, the court dismissed the plaintiffs' First Amendment

---

found that plaintiffs had "failed to allege any 'injury in fact' related to HHS's promulgation of the Privacy Rule," and that plaintiffs thus lacked standing to challenge the

claims for lack of standing.[1/]

The district court then rejected plaintiffs' Tenth Amendment claim on two grounds. First, the court concluded that, under Tennessee Electric Power Co. v. TVA, 306 U.S. 118 (1939), private parties have no standing to sue to enforce the Tenth Amendment. Second, the court concluded that the plaintiffs' Tenth Amendment claim failed even if they did have standing. Explaining that HIPAA "regulates interstate economic activity," because "[h]ealth plans operate across state lines" and because "[h]ealth care providers transmitting health information . . . also engage in interstate commerce," RE4 at 7, the court held that "HIPAA falls within Congress's Commerce Clause authority." Id.

---

constitutionality of that Rule. Id. at 6.

[8/] The court also rejected the claim by one plaintiff that she had suffered actual injury due to the release of her child's vaccination information under state law. As the court recognized, "the Privacy Rule has no bearing on Texas or other state laws governing the vaccination of children or other health matters. Even if the Privacy Rule were invalidated, state laws would remain in effect, and the disclosures about which plaintiffs complain would continue." Id. at 6-7.

Finally, the district court dismissed each of the plaintiffs' statutory claims. RE4 at 8. The court found that HHS had not exceeded its authority under HIPAA in extending the Privacy Rule to protect the privacy of information contained in non-electronic medical records, that HHS' delay in promulgating the Privacy Rule did not deprive it of power to act, that HHS had not violated the procedural requirements of the Regulatory Flexibility Act, and that plaintiffs had no private right of action under the Paperwork Reduction Act to seek invalidation of the Privacy Rule. Id. at 8-10. On appeal, plaintiffs have abandoned each of these claims except their assertion that HHS violated the RFA.[1/]

STANDARD OF REVIEW

The district court's order of dismissal under Rule 12(b)(1) and 12(b)(6) is reviewed de novo. See Ramming v. United States, 281 F.3d 158, 161 (5th Cir. 2001).

SUMMARY OF ARGUMENT

In enacting HIPAA, Congress sought to improve the efficiency of the health care system by promoting standards for the transfer

[9/] Another district court has also rejected challenges to HIPAA and the Privacy Rule similar to the claims in this case. See South Carolina Medical Assn. v. Department of Health and Human Services, No. 01-2965 (D. S.C. Aug. 14, 2002), appeal pending, No. 02-2001 (4th Cir.).

and storage of health information. Recognizing that increased traffic in medical information could increase the risk that confidential information might be improperly disclosed, Congress also directed HHS to issue rules to protect patient privacy. The Privacy Rule promulgated by HHS secures medical privacy rights by limiting the disclosures of information that health care businesses can undertake without patient permission. It creates a regulatory "floor" of individual privacy rights, not a ceiling, because HIPAA explicitly states that the Rule "shall not supercede" state laws that provide patients with "more stringent" protections than the Rule.

The Privacy Rule permits – but does not require – covered entities to disclose patient information without the patient's authorization in certain circumstances, but only when doing so is either mandated by or consistent with pre-existing state laws. Only one provision of the Rule, 45 C.F.R. § 160.310, establishes a new affirmative obligation to allow governmental access to patient information. If the Secretary decides to investigate a covered entity to ensure that it is complying with the Rule's privacy requirements, the covered entity must provide access to its paper and electronic records. Although HHS may examine those records if the information is deemed "pertinent" to the compliance investigation, that information cannot be released except as part of the government's privacy enforcement efforts or as otherwise required by law. Plaintiffs' constitutional

challenge therefore focuses on a provision designed to protect their privacy, not to undermine it.

1. Plaintiffs seek facial invalidation of the Privacy Rule on the ground that 45 C.F.R. § 160.310 could be employed at some future time in a manner that would result in the disclosure of some private medical information to HHS. As the district court properly concluded, however, plaintiffs' pre-enforcement, facial challenge to the Privacy Rule on First and Fourth Amendment grounds fails for lack of standing and ripeness.

A. Plaintiffs' Fourth Amendment claim fails simply because they have not been subjected to an unlawful "search" or "seizure" of their medical records. Nor can they claim that such a search is imminent, because that presupposes a lengthy and speculative chain of events in which the Secretary of HHS would have to choose to exercise his discretionary authority not only to institute a compliance investigation of a covered entity but also to obtain a plaintiffs' personal information. Fourth Amendment claims are typically evaluated on concrete facts, not conjecture about possible future governmental action. The complete absence of any factual context for the plaintiffs' claims of an "unreasonable search" would make it impossible for the district court to apply the substantive standards of the Fourth Amendment. And, in any event, the remedy for any hypothetical future Fourth Amendment violation would not be the invalidation of the Privacy Rule – as plaintiffs seem to suggest – but rather invalidation of

the specific search at issue. Thus, the district court correctly concluded that plaintiffs' Fourth Amendment claim was not ripe for review and that plaintiffs lacked standing to pursue it.

B. For similar reasons, plaintiffs also lack standing to pursue their pre-enforcement First Amendment challenge to the Privacy Rule. Most importantly, plaintiffs have not alleged any actual or imminent First Amendment injury. The Privacy Rule does not regulate doctor-patient speech, and imposes no penalties on doctors or patients based on the content of their communications. Instead, the sole predicate for plaintiffs' claim of First Amendment injury is an asserted "reluctance" – not an actual refusal – to speak freely with their physicians due to their fear that 45 C.F.R. § 160.310 may be used by HHS in the future to obtain medical records during its efforts to ensure compliance with the Privacy Rule. Given the many ways in which private medical records may already be disclosed under state law, the possibility of one additional limited disclosure to HHS does not pose an objectively reasonable "chill" on plaintiffs' communications with their doctors. Under Laird v. Tatum, 408 U.S. 1 (1972), plaintiffs lack standing to seek facial invalidation of the Privacy Rule based solely on their assertions of a "subjective chill" under the First Amendment.

2. Plaintiffs' Tenth Amendment claim fares no better than their other constitutional claims. Private parties generally do not have standing to press Tenth Amendment claims. To the extent

that plaintiffs' claim is understood as a challenge to Congress's authority under the Commerce Clause to regulate the exchange of medical information between health care businesses, that challenge lacks merit. Regulation of economic activity that has a substantial impact on interstate commerce and routinely involves exchange of information across state lines is plainly within Congress's regulatory authority.

3. Finally, HHS followed all the requirements of the Regulatory Flexibility Act (RFA) when it promulgated the Privacy Rule. That Act imposes requirements that are purely procedural: agencies promulgating rules that affect small businesses must estimate the costs of compliance and consider regulatory alternatives that will decrease those costs. As required by the RFA, HHS published a "final regulatory flexibility analysis" that discussed its cost estimates and the steps it took to reduce the impact of the Privacy Rule on small businesses. That analysis reveals that HHS not only considered, but in some cases adopted rule changes in order to accommodate such concerns. The RFA requires no more.

ARGUMENT

I. PLAINTIFFS' FIRST AND FOURTH AMENDMENT CLAIMS FAIL ON STANDING AND RIPENESS GROUNDS.

A. In order to satisfy the "case or controversy" requirements of Article III of the Constitution, a plaintiff bears the burden of establishing the three elements of standing.

The first of these requirements is that the plaintiff must demonstrate "'injury in fact' – an invasion of a legally protected interest which is (a) concrete and particularized, and (b) 'actual or imminent, not conjectural or hypothetical'" Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (citations omitted). Second, there must be a causal connection between the plaintiff's injury and the defendant's conduct that makes the injury "fairly traceable" to the conduct. Id. And finally, it must be likely, not just speculative, that the plaintiff's injury would be redressed by a favorable decision. Id. at 561.

An Article III case or controversy must be brought not only by an appropriate plaintiff, but at an appropriate time. The ripeness doctrine limits the jurisdiction of the federal courts by avoiding adjudication of abstract controversies in the absence of concrete hardship. The Supreme Court explained in Abbott Laboratories v. Gardner, 387 U.S. 136 (1967), that the basic rationale of the ripeness doctrine is

> to prevent the courts, through avoidance of premature adjudication, from entangling themselves in abstract disagreements over administrative policies, and also to protect the agencies from judicial interference until an administrative decision has been formalized and its effects felt in a concrete way by the challenging parties.

Id. at 148-49; accord Pennzoil Co. v. FERC, 742 F.2d 242, 244 (5th Cir. 1984). The Court set out a two-part test for determining ripeness, observing that it would consider "the fitness of the issues for judicial decision" as well as "the

hardship to the parties of withholding court consideration." 387 U.S. at 149.

Applying these standards, the courts have recognized that review of final agency action is precluded – even where it involves pure questions of law – when the effects of the action have not been felt and the denial of review results in little or no hardship. For example, in Toilet Goods Ass'n v. Gardner, 387 U.S. 158 (1967), the Supreme Court found unripe a facial challenge to a regulation even though the petitioners' contention was that the regulation was "totally beyond the agency's power under the statute." Id. at 163. See also Pennzoil, 742 F.2d at 245 (review of "purely legal" question unripe for review in absence of direct and immediate impact); McCarthy v. Briscoe, 553 F.2d 1005, 1007 (5th Cir. 1977) (challenge to statute unripe where enforcement is speculative).

B. Application of these standards makes plain that plaintiffs have demonstrated neither the elements of standing nor the ripeness of their claims.

The gravamen of plaintiffs' claims is that the Privacy Rule may result in a search barred by the Fourth Amendment or chill doctor-patient discussions. At the outset, it should be noted that section 264 of HIPAA and the Privacy Rule are designed to protect medical privacy. As Congress explained, "[p]rotecting the privacy of individuals is paramount." H. Rep. No. 104-496, 104th Cong., 2d Sess. at 100 (1996), reprinted in 1996

U.S.C.A.A.N. at 1900. That concern is reflected throughout the Privacy Rule, which provides as a general matter that a covered entity "may not use or disclose protected health information" without a valid and affirmative authorization by the patient, and establishes specific and limited exceptions to that rule. See 45 C.F.R. § 164.502 et seq.

The Privacy Rule establishes a regulatory "floor" of medical privacy protection without creating a ceiling of privacy rights. HIPAA's non-preemption provision states that the Rule "shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent" than those imposed by the Rule. 42 U.S.C. § 1320d-2 note (c)(2) (emphasis added); see also 45 C.F.R. § 160.202 (a "more stringent" law is, in general, one that "provides greater privacy protection for the individual" or greater rights of access for the individual). The Act thus preserves any state-created privacy protection that existed prior to its passage.

Existing state laws routinely require disclosures of private medical information. The Supreme Court has noted that

> disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient.

Whalen v. Roe, 429 U.S. 589, 602 (1977) (emphasis added). In some cases, state laws allow disclosure as a matter of common

sense – for example, when they allow doctors to disclose an individual's private health information in the course of treating the individual during an emergency. In others, state laws require or allow disclosure as a matter of public health policy – for example, by allowing state officials to track the spread of infectious disease, or by requiring doctors to report suspected instances of child abuse. The Privacy Rule creates exceptions to its general non-disclosure rule to accommodate these state law concerns, see, e.g., 45 C.F.R. § 164.512, but it does not require any such disclosures.

In sum, patients have at no time had an absolute expectation of privacy in their medical records. Disclosures have always been authorized under state law. The Privacy Rule preserves existing state law restrictions on disclosure while providing additional protections.

C. Plaintiffs assert that they are harmed by a provision of the Privacy Rule, 45 C.F.R. § 160.310, which requires entities covered by the Rule to disclose protected health information when such information is relevant to HHS' Privacy Rule enforcement efforts. This is the only provision of the Privacy Rule that establishes a new requirement of mandatory disclosure to the government. See RE4, at 5 n.4 ("Most of the regulations about which the plaintiffs complain do not mandate disclosures to the government, but merely permit entities, without violating the

Privacy Rule, to comply with state and federal laws that already require disclosure of protected health information.") (emphasis added). As described earlier, a covered entity must cooperate with HHS "if the Secretary undertakes an investigation" of a covered entity to determine whether it is complying with the Privacy Rule. 45 C.F.R. § 160.310(b) (emphasis added). In the course of such an investigation, the Secretary may request disclosure of records that contain protected health information, so long as that information is "pertinent to ascertaining compliance" with HIPAA and the Privacy Rule. Id. § 160.310(c)(1). The Secretary is then forbidden to disclose this information "except if necessary for ascertaining or enforcing compliance" or as otherwise required by law. Id. § 160.310(c)(3); see also 5 U.S.C. § 552a (generally prohibiting agency disclosure of individual information in government records). Plaintiffs believe that the mere existence of this rule constitutes an Article III injury and that their claims are ripe for review. The district court correctly concluded otherwise.

1. Fourth Amendment Claim

Plaintiffs cannot claim that their medical information has been "searched" or "seized" in a manner that causes a cognizable Fourth Amendment harm. Plaintiffs therefore allege that they fear they might be searched at some point in the future. But Fourth Amendment claims asserting the "unreasonableness" of a

search are generally evaluated on a case-by-case basis, in which courts weigh the asserted governmental interests against the particular invasion of the individual's privacy established by the facts of the case. See Terry v. Ohio, 392 U.S. 1, 17-18, n. 15 (1968). Moreover, the judicial remedy that normally results — exclusion of evidence from a legal proceeding – is not the remedy plaintiffs seek. They seek to have portions of the Privacy Rule struck down in their entirety. Plaintiffs' Fourth Amendment claim therefore comes before this court in a highly unusual posture: to succeed, they must demonstrate that the enforcement provision of the Privacy Rule can never be applied in a constitutionally permissible manner – without any evidence as to how the Rule has actually been applied. See United States v. Salerno, 481 U.S. 739, 745 (1987) (in facial challenges outside the First Amendment, "the challenger must establish that no set of circumstances exists under which the Act would be valid").

After the compliance dates for the Privacy Rule,[10/] a chain of increasingly unlikely events would have to take place before plaintiffs could suffer any cognizable Fourth Amendment injury. The Secretary would have to implement an enforcement program to police compliance with the Privacy Rule. He would then have to investigate a covered entity that retains records containing protected information about one of the plaintiffs. Next, the

[10/] The compliance dates are April 14, 2004 for small health plans and April 14, 2003 for other covered entities.

Secretary would have to request those records in the course of his compliance investigation, relying exclusively upon his authority under 45 C.F.R. § 160.310(c)(1) and not his administrative subpoena power under 42 U.S.C. §§ 405(d)-(e), 1320d-5(a)(2), and 1320a-7a.[1/] The Secretary would then have to find that one of the plaintiffs' personal medical information was "pertinent to ascertaining compliance." And finally, the Secretary would have to access that private information in a manner that somehow constituted an "unreasonable search" under the Fourth Amendment. See Trustees for Alaska v. EPA, 749 F.2d 550, 560 (9th Cir. 1984) (dismissing claim that administrative enforcement provision was unconstitutional because plaintiffs "ha[d] not even alleged that any search ha[d] occurred").

An injury so speculative cannot create Article III standing. See City of Los Angeles v. Lyons, 461 U.S. 95, 108 (1983) (no case or controversy where it was "no more than conjecture" that plaintiff would be injured by assertedly unconstitutional police practices). Plaintiffs' claim therefore parallels the claim held unripe in United Transportation Union v. Foster, 205 F.3d 851 (5th Cir. 2000). There, this Court rejected a request for pre-enforcement review of a law mandating drug testing of railroad crews after rail collisions even when investigators lacked

[11/] The Secretary's use of this administrative power has been upheld in Doe v. United States, 253 F.3d 256 (6th Cir. 2001).

probable cause. This court recognized that a number of events would have to take place in order for an actual search to take place. First, a train collision would have to occur. Second, to trigger the law, an investigating officer would have to find "reasonable grounds" to believe that train operators were under the influence of drugs or alcohol. Third, the investigating officer would have to determine that "reasonable grounds" meant something less than "probable cause," and fourth, actual probable cause would have to be absent. This Court refused to assume the inevitability of this causal chain, and instead held that the case was properly dismissed because of its "extreme prematurity." Id. at 858. As in United Transportation Union, the Fourth Amendment claim in this case concerns matters that are "hypothetical, conjectural, conditional, or based upon the possibility of a factual situation that may never develop." Rowan Companies, Inc. v. Griffin, 876 F.2d 26, 28 (5th Cir. 1989) (citation omitted).

A Fourth Amendment challenge to the Privacy Rule cannot properly be assessed absent a more concrete setting. The standards that guide Fourth Amendment inquiries are "fluid concepts that take their substantive content from the particular contexts in which the standards are being assessed," Ornelas v. United States, 517 U.S. 690, 696 (1996), and the Supreme Court has directed that "[e]ach case is to be decided on its own facts and circumstances." Ker v. California, 374 U.S. 23, 33 (1963)

(citations omitted). As a result, the Court has previously recognized that "[i]n a pre-enforcement challenge it is difficult to determine whether Fourth Amendment rights are seriously threatened." Village of Hoffman Estates v. Flipside, 455 U.S. 489, 504 n.22 (1982). Requiring the district court immediately to rule on the validity of 45 C.F.R. § 160.310 would both force it to act without "an actual factual setting that makes such a decision necessary," and deprive it of the very information it needs to make that considered constitutional judgment. Hodel v. Virginia Surface Mining & Reclamation Assn., Inc., 452 U.S. 264, 294-95 (1981). The district court thus properly refused to adjudicate plaintiffs' Fourth Amendment claim.

2. First Amendment

The district court also properly concluded that plaintiffs' First Amendment claim should be dismissed. Plaintiffs premise their First Amendment claim on an asserted "reluctance" to speak freely with their doctors due to the incremental privacy loss associated with HHS' potential use of 45 C.F.R. § 160.310. As discussed, however, disclosures of medical information have always been required under state law, and plaintiffs' claim of chill from the possibility of one additional form of disclosure under the Privacy Rule is therefore not objectively reasonable.

Plaintiffs do not allege that the Privacy Rule regulates communications between doctors and patients, nor that it threatens them with any potential penalties based on the content

of such speech. Instead, plaintiffs suggest that their speech may be chilled because they fear possible disclosures of their private medical information under the Privacy Rule. But state reporting laws and the myriad disclosures that occur in the routine course of medical care constitute far greater intrusions upon privacy.[12] Plaintiffs cannot seek facial invalidation of the Privacy Rule on the ground that it leaves in place state laws permitting such disclosures. Nor can they assert any "objective chill" from the possibility of one additional form of disclosure under the Privacy Rule. Cf. New Hampshire Right to Life Political Action Committee v. Gardner, 99 F.3d 8, 14 (1st Cir. 1996) ("A party's subjective fear that she may be prosecuted for engaging in expressive activity will not be held to constitute an injury for standing purposes unless that fear is objectively reasonable.").

The Supreme Court's analysis in Laird v. Tatum, 408 U.S. 1 (1972), makes clear that plaintiffs' allegations fail to establish a First Amendment claim. In that case, plaintiffs challenged the constitutionality of an Army surveillance program

[12] Two of the plaintiffs' own affidavits prove this point. Plaintiffs Dawn Richardson and Melvin E. Edwards allege injuries that stem from the activities of state officials in Texas. These activities would continue even if the Privacy Rule were struck down in its entirety. See RE7, RE13.

designed to monitor civilian activities, claiming that the mere existence of the program made them less willing to speak freely. Plaintiffs admitted, however, that they had not been the targets of any specific surveillance, and the Court rejected the contention that their "chill" sufficed to create a justiciable First Amendment controversy. Chief Justice Burger, writing for the Court, recognized that other Supreme Court cases had found cognizable First Amendment injuries arising from the deterrent or "chilling" effect of regulations. But, as he explained:

> In none of these cases . . . did the chilling effect arise merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some other and additional action detrimental to that individual.

Id. at 11 (collecting cases); see also United Presbyterian Church v. Reagan, 738 F.2d 1375, 1378-79 (D.C. Cir. 1984) (in "chilling effect" cases, the "chill" is the "reason why the governmental imposition is invalid rather than . . . the harm which entitles the plaintiff to challenge it"). In the absence of any immediate harm or threat of future harm based on the content of the plaintiffs' speech, the only injuries the Laird plaintiffs could allege were their discomfort with the Army's activities and their "speculative apprehensiveness that [the government] may at some

future date misuse the information in some way that would cause direct harm." 408 U.S. at 13. The Chief Justice described such concerns as a "subjective chill." Id. He then flatly declared that, in the First Amendment context, allegations of subjective chill "are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm." Id. at 14; see also Meese v. Keene, 481 U.S. 465, 473 (1987) (film exhibitor required to show "cognizable injury" beyond a "subjective chill" to establish standing).

Just as in Laird, the only First Amendment injury alleged by the plaintiffs in this case is a "subjective chill." None of them suggests that HHS has accessed their private medical information, nor can they establish with any degree of certainty that their personal information will ever be accessed. And, under Laird, their discomfort with the Privacy Rule and "speculative apprehensiveness" of future government misconduct relating to its enforcement do not constitute a cognizable First Amendment injury. See National Council for Improved Health v. Shalala, 122 F.3d 878, 884 n.9 (10th Cir. 1997) ("An allegation of inhibition of speech, without more, will not support standing.") (citing Laird, 408 U.S. at 13-14); United States v. Ramsey, 503 F.2d 524, 526 n.5 (7th Cir. 1974) (dismissing plaintiffs' argument that mere existence of federal wiretapping statute could "chill" protected speech). As a result, the plaintiffs cannot satisfy either of the two prongs of the "injury

in fact" requirement; their asserted injury is neither "concrete and particularized" nor "actual or imminent." Lujan, 504 U.S. at 560.

The plaintiffs' other asserted injuries do no more to establish their claim to First Amendment standing. For example, the doctor plaintiffs allege that they will be injured when they are forced to spend significant sums to comply with the Privacy Rule. But they say nothing about how this injury could be redressed by striking down a provision of the Rule that allows HHS to enforce substantive privacy protections. To lift the doctors' financial burden, the court would have to strike down the provisions of the Privacy Rule that protect patient privacy by requiring doctors to adhere to strict anti-disclosure requirements. See Lujan, 504 U.S. at 561 (discussing requirement of redressability). Plaintiffs have made no First Amendment challenge to those provisions.

The patient plaintiffs contend that their market choice is in some way curtailed by the Privacy Rule. But the government often issues regulations that have significant effects on market choice, and none of these is viewed as inflicting First Amendment harm. If Congress were, for example, to pass a law immediately abolishing Medicare, it would no doubt impair the plaintiffs' medical care options. But that impairment could not reasonably confer standing to challenge the law under the First Amendment. And in any case, it is objectively implausible that the

plaintiffs' privacy is meaningfully reduced by the single disclosure requirement of the Privacy Rule of which they complain. Taken seriously, the plaintiffs' concerns should also lead them to avoid seeking federal disability and Medicare benefits, because such statutes require disclosure to the government of sensitive medical information. Yet they raise no First Amendment objections to those statutes nor suggest cases in which such challenges have been successful.

Finally, the plaintiffs' near-exclusive reliance upon Whalen v. Roe, 429 U.S. at 589, is misplaced. That case never analyzed the issue of whether its patient plaintiffs had standing, and it thus has no precedential value in a case where standing is contested. See Steel Co. v. Citizens for a Better Environment, 523 U.S. 83, 91 (1998) ("drive-by jurisdictional rulings . . . have no precedential effect"). Moreover, Whalen involved a statute that had concrete effects upon the plaintiffs. The New York law at issue in that case required doctors to provide the State with a copy of every prescription they wrote for certain drugs. The State maintained that information in a central database and used it to detect and investigate patients, doctors, or pharmacists who unscrupulously used, prescribed, or sold drugs. There was no dispute that the plaintiffs' records would inevitably be incorporated into the database and reviewed by government officials. The plaintiffs in Whalen could therefore allege immediate and concrete "injuries in fact": one had stopped

taking a regulated medication as a result of the statute. 429 U.S. at 595 n.16. They were not forced to rely upon allegations of "subjective chill" resulting from a chain of events that might result in a disclosure of some private medical information at some point in the future.

The true relevance of Whalen to the present case is that the Court found that disclosures of private health information to state officials did not threaten constitutional harm:

> Such disclosures [are not] meaningfully distinguishable from a host of other unpleasant invasions of privacy that are associated with many facets of health care. Unquestionably, some individuals' concern for their own privacy may lead them to avoid or to postpone needed medical attention. Nevertheless, disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient. Requiring such disclosures to representatives of the State having responsibility for the health of the community, does not automatically amount to an impermissible invasion of privacy.

Id. at 602 (emphasis added).[1/] Whalen therefore shows that the plaintiffs cannot allege any cognizable injury arising out of the limited disclosure of their medical information to HHS. The

[13/] This discussion also explains why the plaintiffs are mistaken in asserting that the Privacy Rule forces physicians to violate their Hippocratic Oath. Doctors are not expected to keep patient information absolutely secret; disclosures of such information are an "essential part of modern medical practice." See also 429 U.S. at 602 n.28 ("The physician-patient privilege is unknown to the common law. In States where it exists by legislative enactment, it is subject to many exceptions and to waiver for many reasons.") (citations omitted).

district court was thus correct to dismiss the plaintiffs' First and Fourth Amendment claims.

II. PLAINTIFFS' TENTH AMENDMENT CLAIM WAS PROPERLY DISMISSED.

Plaintiffs' remaining constitutional claim is that HIPAA violates the Tenth Amendment by regulating the privacy of individually identifiable health information that is not exchanged across state boundaries.

As a threshold matter, it is not precisely clear what plaintiffs assert in their Tenth Amendment claim. Plaintiffs have standing to pursue their Tenth Amendment claim only to the extent that they contend that HIPAA's provisions fall outside Congress' Commerce Clause authority. The federal courts routinely entertain claims of this sort. See, e.g., United States v. Lopez, 514 U.S. 549 (1995). But in this case, plaintiffs' Commerce Clause challenge fails because the use and disclosure of private medical information is an activity that has a "substantial relation" to interstate commerce, and can therefore be regulated by Congress under the Commerce Clause. Id. at 559.

The businesses that HIPAA covers – health insurance plans, health care providers, and health care clearinghouses – are routine participants in interstate commerce. Subtitle F of HIPAA, at issue in this case, requires HHS to adopt standards for certain electronic health care transactions and data elements in order to encourage those businesses to conduct health care

transactions using such media. Those transactions are commercial in nature, and will often be conducted between entities in different States. See 42 U.S.C. § 1320d-2(a) (listing health plan enrollments, premium payments, and insurance claims as among the "financial and administrative" transactions regulated).

In order to avert threats to the confidentiality of health information that will be exchanged or retained by health care businesses, Subtitle F also required HHS to develop privacy standards that would complement the new information standards. See 42 U.S.C. § 1320d-2 note (c). The relationships between these privacy standards and interstate health care commerce are numerous and direct. For example, patients who are concerned that health care businesses will reveal their private information may delay medical attention or hesitate to disclose pertinent medical history. Such actions will directly affect health care insurance costs nationwide. See United States v. Evans, 928 F.2d 858, 862 (9th Cir. 1991) (federal regulation of machine guns permissible because of nationwide effects on insurance).

In addition, the conversion to electronic health care information transactions may be delayed if patients perceive that the system threatens their privacy. Such delays would hamper the nationwide efficiency gains that Congress sought to achieve through that conversion. See H. Rep. No. 104-496, 104th Cong., 2d Sess. at 97, reprinted in 1996 U.S.C.A.A.N. at 1898 (estimating five-year savings of over $29 billion from HIPAA

compliance). Also, medical privacy is an important issue in the context of employment: the protections created by the Privacy Rule will limit the access of employers to medical information during their evaluations of current or prospective employees. The use and disclosure of confidential medical information is thus an activity that "substantially affects" interstate commerce, and plaintiffs cannot plausibly claim that HIPAA exceeds Congress' authority under the Commerce Clause. Cf. Reno v. Condon, 528 U.S. 141, 148-49 (2000) (upholding federal restrictions on state disclosure of driver registration information against Tenth Amendment and Commerce Clause challenges).

It is possible that the plaintiffs seek to assert a different kind of Tenth Amendment claim, in which they contend that HIPAA impermissibly interferes with state governance or improperly commandeers state officials to carry out federal regulatory goals. But aside from a few passing allegations in their complaint, plaintiffs have said nothing to explain what the nature of this claim might be. That is because neither HIPAA nor the Privacy Rule "compel[s] the States to enact or administer a federal regulatory program." Printz v. United States, 521 U.S. 898, 933 (1997) (quoting New York v. United States, 505 U.S. 144, 188 (1992)).

In any event, the plaintiffs lack standing to pursue this sort of Tenth Amendment claim. In Tennessee Electric Power Co.

v. TVA, the Supreme Court stated in unambiguous terms that private parties lack standing to sue to vindicate the rights of the states if a State or state officer does not join the suit. 306 U.S. at 144. In that case, a number of public utility corporations sued to prevent the newly-created Tennessee Valley Authority (TVA) from competing with them by generating or selling electricity. The utilities alleged, among other things, that the statute creating the TVA violated the Tenth Amendment by "permitting federal regulation of purely local matters reserved to the states or the people by the Tenth Amendment." Id. at 143. The Supreme Court affirmed the district court's dismissal of this claim, stating that "the appellants, absent the states or their officers, have no standing in this suit to raise any question under the amendment." Id. at 144.

Like the plaintiffs in Tennessee Electric, plaintiffs here cannot show that the State of Texas considers HIPAA an impermissible interference in its affairs. Indeed, such an objection would be surprising in light of HIPAA's explicit preservation of contrary state privacy rules that are "more stringent" than the federal provisions. 42 U.S.C. § 1320d-2 note (c)(2). Thus, plaintiffs lack standing to pursue a claim that the Privacy Rule commandeers state resources in violation of the Tenth Amendment.[14/]

[14/] Although other courts have questioned whether Tennessee Electric precludes standing for private parties asserting Tenth

III. HHS COMPLIED WITH THE REQUIREMENTS OF THE REGULATORY FLEXIBILITY ACT.

The Regulatory Flexibility Act (RFA) requires any agency promulgating a rule that will have a "significant impact" on "small entities" to publish an "initial regulatory flexibility analysis" that describes the rule's impact. 5 U.S.C. § 603. After a public comment period, the agency must then publish a "final regulatory flexibility analysis" (FRFA) along with its final rule. 5 U.S.C. § 604. The FRFA must contain several elements, most importantly:

> a description of the steps the agency has taken to minimize the significant economic impact on small entities consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected.

Id. § 604(a)(5). These requirements are "purely procedural," United States Cellular Corp. v. F.C.C., 254 F.3d 78, 88 (D.C. Cir. 2001), and judicial review of agency compliance exists "only

---

Amendment claims, see, e.g., Gillespie v. City of Indianapolis, 185 F.3d 693, 700-03 (7th Cir. 1999); Seniors Civil Liberties Assn. v. Kemp, 965 F.2d 1030, 1033 n.6 (11th Cir. 1992), this Court has previously affirmed another district court that followed its holding. See Gaubert v. Denton, 1999 WL 350103 at *5 (E.D. La. 1999), aff'd 210 F.3d 368 (5th Cir. 2000).

to determine whether an agency has made a 'reasonable, good-faith effort' to carry out [its] mandate." Alenco Comm., Inc. v. FCC, 201 F.3d 608, 625 (5th Cir. 2000) (quoting Associated Fisheries of Maine, Inc. v. Daley, 127 F.3d 104, 114 (1st Cir. 1997)).

HHS complied with the requirements of the RFA by publishing a FRFA for the Privacy Rule, which appears at 65 Fed. Reg. 82462, 82779-93. This FRFA satisfies statutory requirements by addressing the following issues:

> (1) The need for, and objective of, the rule; (2) a summary of the public comments to the NPRM and the Department's response; (3) a description and estimate of the number of small entities affected by the rule; and (4) a description of the steps the agency has taken to minimize the economic impact on small entities, consistent with the law and the intent of the rule. . . . A description of the projected reporting and record keeping requirements of the rule are included in Section IX, below.

65 Fed. Reg. 82779. In the FRFA, HHS describes its consideration of regulatory alternatives that might reduce the burdens on small businesses. Some of these alternatives were adopted. See e.g., 65 Fed. Reg. 82783 (describing modification of training and recertification requirements "to ease the burden on small businesses"). Others were not, because HHS judged that they would undermine the goals of HIPAA. See, e.g., 65 Fed. Reg. 82779 (rejecting broad exemptions for small businesses that would "essentially nullify the purpose of the rule"); see generally Associated Fisheries, 127 F.3d at 114 ("Congress emphasized that the RFA should not be construed to undermine other legislatively mandated goals."). The FRFA also refers readers to other agency

deliberations regarding small business. See, e.g., 65 Fed. Reg 82641 (discussing rule modifications that ease monitoring burdens on small businesses); id. at 82756 (responding to comments on effects on small businesses). It demonstrates that HHS considered, discussed, and, in some cases, implemented rule modifications that ease the impact of the Privacy Rule upon small businesses. In the words of the Alenco court, "[t]he RFA requires no more." 201 F.3d at 625.

CONCLUSION

For the foregoing reasons, the order of the district court dismissing the complaint should be affirmed.

Respectfully submitted,

ROBERT D. McCALLUM, JR.
Assistant Attorney General

MICHAEL B. SHELBY
United States Attorney

MARK B. STERN
(202) 514-5089
CHARLES W. SCARBOROUGH
(202) 514-1927
SAMBHAV N. SANKAR
(202) 514-0236
Attorneys, Appellate Staff
Civil Division, Room 9108
Department of Justice
601 "D" Street, N.W.
Washington, D.C. 20530

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

CASES:

FEDERAL STATUTES:

REGULATIONS:

RULES:

ADMINISTRATIVE MATERIALS:

LEGISLATIVE MATERIALS:

CERTIFICATE OF INTERESTED PERSONS

The undersigned counsel of record certifies that there are no additional interested parties other than the ones listed by appellants.

_____

SAMBHAV N. SANKAR
Attorney for the Appellee

STATEMENT REGARDING ORAL ARGUMENT

Appellees believe that the judgment of the district court is correct and should be affirmed. We stand ready to present oral argument if the Court would find argument to be of assistance.

CERTIFICATE OF SERVICE

I hereby certify that on this 14th day of November 2002, I served the foregoing BRIEF FOR APPELLEES, along with a virus-fee computer diskette containing the full text of the brief, upon the clerk of the Court of Appeals and upon counsel of record, by causing copies to be sent by United States Mail, postage prepaid, to:

Andrew Layton Schlafly
AAPS General Counsel
939 Old Chester Road
Far Hills NJ 07931

Karen Bryant Tripp
2245 Shakespeare
Houston TX 77030

_____
SAMBHAV N. SANKAR
Attorney for the Appellee

CERTIFICATE OF COMPLIANCE

In accordance with Fed. R. App. P. 32(a)(7)(C), I hereby certify that the foregoing Brief for the Defendants-Appellees is monospaced in 12-point Courier font and was produced on Corel Wordperfect 9. Exclusive of the portions exempted by Fed. R. App. P. 32(a)(7)(B)(iii), this brief contains 9016 words, according to Corel Wordperfect 9.

_____

SAMBHAV N. SANKAR
Attorney for the Appellee