09-1913-cv(L)

09-2056-cv(CON)

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

IMS HEALTH INCORPORATED, VERISPAN, LLC, SOURCE HEALTHCARE ANALYTICS, INC., a subsidiary of Wolters Kluwer Health, Inc., and PHARMACEUTICAL RESEARCH AND MANUFACTURERS OF AMERICA,
Plaintiffs-Appellants,

v.

WILLIAM H. SORRELL, as Attorney General of the State of Vermont, JIM DOUGLAS, in his official Capacity as Governor of the State of Vermont, and ROBERT HOFMANN, in his capacity as Secretary of the Agency of Human Services of the State of Vermont,
Defendants-Appellees.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF VERMONT

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLEE AND URGING AFFIRMANCE

Marc Rotenberg
Motion for Admission Pending
Counsel of Record
John Verdi
Jared Kaprove (Va. Admission Pending)
Kim Nguyen (Md. Admission Pending)
Electronic Privacy
Information Center (EPIC)
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

September 15, 2009

CORPORATE DISCLOSURE STATEMENT
Purusuant to Fed. R. App. P. 26.1 and 29(c)
for Case No. 09-1913-cv(L)

Amicus Curiae, Electronic Privacy Information Center ("EPIC"), is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of the stock of EPIC.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

State Cases

Federal Statutes

State Statutes

Federal Regulations

Other Authorities

STATEMENT OF AMICUS

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values. EPIC has participated as *amicus curiae* in several cases before the United States Supreme Court and other courts concerning privacy issues, new technologies, and Constitutional interests, including *Flores-Figueroa v. United States*, 129 S. Ct. 1886 (2009) *Herring v. United States*, 129 S. Ct. 695 (2009); *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008); *Hiibel v. Sixth Judicial Circuit of Nevada*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Department of Justice v. City of Chicago*, 537 U.S. 1229 (2003); *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000); *National Cable and Telecommunications Association v. Federal Communications Commission*, 555 F.3d 996 (D.C. Cir. 2009); *Bunnell v. Motion Picture Association of America*, No. 07-56640 (9th Cir. filed Nov. 12, 2007); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006) 470 F.3d

1104 (5th Cir. 2006); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004), *cert. denied* 544 U.S. 924 (2005); and *State v. Raines*, 857 A.2d 19 (Md. 2003). EPIC has a particular interest in protections that limit disclosure of medical information, and has filed as *amicus* in a case that upheld New Hampshire's prescription privacy law. *See IMS Health v. Ayotte*, 550 F.3d 42 (1st Cir. 2008) *cert. denied* 129 S. Ct. 2864 (2009).

At issue in this case are the privacy interests of Vermont residents that the state of Vermont sought to protect through the enactment of legislation. The state has a vital interest in regulating conduct that enables the transfer and sale of personal medical record information. Not only has Appellant IMS Health challenged this regulation as a violation of Appellant's right to profit from the sale of this sensitive data, Appellant engages in practices that continue to endanger the privacy interests of Vermont residents. *Amicus* therefore submits this brief to make clear the substantial interest in safeguarding sensitive personal information as well as the related concern about the transfer of "anonymized" patient data to datamining firms.

EPIC supports the outcome reached by the district court. In fact, EPIC believes that the court did no go far enough in stating the extent

of the privacy interest at issue in this statute now under consideration by this Court. It is the nature of rapid technological change that the risks to personal privacy are often greater than can be readily understood. This brief of *amicus* EPIC shows that in addition to the concerns expressed about the privacy of prescriber data, there are also substantial concerns for the privacy of patient data. Further, the techniques for anonymity contemplated in the statute are not adequately enforced to safeguard these interests. For these reasons, EPIC urges affirmance of the lower court's decision to uphold the Vermont law.

All parties have consented to the filing of this brief. Fed. R. App. P. 29(a).

ARGUMENT

I. Medical Privacy is a Fundamental Concern for Patients.

There are approximately 1.4 million health care providers in the United States. *IMS Health Inc. v. Ayotte*, 490 F. Supp. 2d 163, 165 (D. N.H. 2007). These providers write billions of prescriptions each year for more than 8,000 different pharmaceutical products. *Id.* These prescriptions are filled at 54,000 retail pharmacies throughout the country. *Id.* The retail pharmacies acquire records for every prescription they fill. These records include: patient name; prescriber identification; drug name; dosage requirement; quantity; and date filled. *Id.* In order to comply with federal and state privacy laws, patient-identifying information is encrypted and de-identified, often with software installed by the datamining companies themselves. *Id.* at 166. The rest of the prescription record remains intact. Thus, a patient's entire drug history is correlated, and each provider can be identified along with their prescribing habits. *Id.* This practice raises privacy concerns for both patients and health care providers.

Public sentiment overwhelmingly favors the protection of patient privacy. Over 70% of the Americans have concerns over the disclosure of

their medical information without their knowledge. Harris Interactive, *HIPAA Notices Have Improved Public's Confidence That Their Medical Information is Being Handled Properly: However public split on benefits of and privacy risks associated with Electronic Medical Records*, Feb. 24, 2005.

Arizona, the District of Columbia, Illinois, Kansas, Maine, Massachusetts, Nevada, New Hampshire, New York, North Carolina, Rhode Island, Texas, Washington, and West Virginia have all considered or enacted bills banning the sale of prescriber data. *See* Ariz. Rev. Stat. Ann. § 32-1973 (2009); D.C. Code § 3-1207.41 (2008); H.B 1459, 95th Gen. Assem. (Ill. 2007); S.B. 229 (Kan. 2007); Me. Rev. Stat. Ann. tit. 22, § 1711-E (2005); S.B. 266 (Md. 2007); S.B. 1275 (Mass. 2007); S.B. 231 (Nev. 2007); N.H. Rev. Stat. Ann. §§ 318:47-f, 318-47g, 318-B:12 (2006); H.B. 5891B, Reg. Sess. (N.Y. 2009); S.B. 159, Gen. Assem. (N.C. 2007); S.B. 2683, Gen. Assem. (R.I. 2008); S.B. 1620 (Tex. 2007); H.B. 1850 (Wash. 2008); W. Va. Code. § 30-5-12c (2008). *See also* Joe Mullin, *States Consider Limits on Medical Data-mining*, Boston Globe, Apr. 7, 2007; The Prescription Project, *Prescription Data Mining*

Fact Sheet, Nov. 19, 2008.[1] Vermont's prescription privacy law bans the sale of prescriber data and is the focus in this case. *See* Vt. Stat. Ann. Tit. 18, § 4631 (2009).

Doctors have also petitioned the American Medical Association (AMA) on behalf of themselves and their patients for legal relief, blaming data-mining companies for interfering with the patient-doctor relationship and violating doctors' and patients' privacy. Tanya Alberts, *Doctors Ask AMA to Assure Some Privacy for their Prescription Pads*, AMNews, Dec. 25, 2000. Even after the AMA adopted an opt-out approach to the sale of prescriber data, doctors continue to question this practice and lobby for stronger safeguards of patient information. Joe Mullin, *States Consider Limits on Medical Data-mining*, Boston Globe, Apr. 7, 2007. The Vermont Medical Society, which represents two-thirds of doctors practicing in Vermont, unanimously passed a resolution asserting that "the use of physician prescription information by sales representatives is an intrusion into the way physicians practice medicine." Vt. Stat. Ann. tit. 33, § 1998(20) (2009).

Although the AMA's Prescribing Data Restriction Program

---

[1] *Available at* http://www.prescriptionproject.org/tools/fact_sheets/files/0004.pdf.

(PDRP) allows physicians to opt out of having their prescribing history accessed by drug representatives, many physicians feel it is inadequate. The National Physician's Alliance supports a complete ban on the sale of prescriber data. Nat'l Physician's Alliance, *Issue Brief: The Sale of Physician Prescribing Data Raises Health Care Costs* (Feb. 2009).[2] They have spoken against the PDRP because the program is burdensome and not widely publicized. Further, even if a physician opts out, there is no guarantee that AMA will not sell prescriber data to pharmaceutical companies. The opt-out only means pharmaceutical companies agree to restrict the sale or release of the data to their drug detailers, although the policy does not provide patients or physicians with a clear legal remedy if a company fails to comply. *Id.*

Health care providers face the unique challenge of providing quality, affordable health care to everyone, while protecting each patient's fundamental right to privacy. The increasing use of electronic databases of patient information could meet many of these goals by reducing institutional costs, integrating applicable data from multiple sources, and allowing patients to receive a higher and more accurate

[2] *Available at* ttp://npalliance.org/images/uploads/IssueBrief-Prescribing_Data_low_res.pdf.

level of care. *See* Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J. Law, Med., & Ethics 98, 98-99 (1997) (summarizing industry and research use of personally identifiable health care information). However, this transition to a centralized depository for health care information requires the disclosure of private medical records to secondary actors, such as researchers, economists, statisticians, administrators, consultants, and computer scientists. Unfortunately, the current legal and security infrastructure surrounding patient medical information has not undergone a similar modernization for the electronic age. As a result, electronic health care records systems and centralized health care databases lack meaningful privacy safeguards.

II. The Vermont Act Relating to Increasing Transparency of Prescription Drug Pricing and Information Advances a Substantial State Interest in Privacy Protection.

For the reasons set forth above and in the brief of Appellee William H. Sorrell, the Attorney General for the State of Vermont, the Vermont legislature passed Senate Bill 115 to protect the public health of Vermont citizens, protect the privacy of prescribers and prescribing information, and to contain costs in the private health care sector.

It is the provision of the Act that permits marketing use of "patient and prescriber data" that "does not identify a prescriber and [for which] there is no reasonable basis to believe that the data provided could be used to identify a prescriber" that gives rise to EPIC's brief. 18 Vt. Stat. Ann. tit. 18, § 4631 (2007). Simply stated, the privacy interest that undergirds the state's interest in this statute is even greater than what the legislature expressly recognized in the findings. Further, IMS Health's asserted safeguards regarding prescriber-identifiable information and de-identified patient data are neither efficient nor strong enough to protect the privacy interests of patients and doctors or to preserve doctor-patient confidentiality. The Court should give great weight to patients' privacy interests in its *Central Hudson* analysis. *See Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557 (1980).

As Judge Posner wrote for the Seventh Circuit in *Northwestern Memorial Hospital v. Ashcroft*, 362 F.3d 923 (7th Cir. 2004), a case involving access to redacted medical records:

> Even if there were no possibility that a patient's identity might be learned from a redacted medical record, there would be an invasion of privacy. Imagine if nude pictures of

> a woman, uploaded to the Internet without her consent though without identifying her by name, were downloaded in a foreign country by people who will never meet her. She would still feel that her privacy had been invaded. The revelation of the intimate details contained in the record of a late-term abortion may inflict a similar wound.

Professor Jerry Kang has explained:

> [W]e must recognize that anonymity comes in shades. Although no specific individual is identified facially, the individual may be identifiable in context or with additional research. . . . Imagine that a psychiatrist publishes verbatim counseling notes in a best-selling book, but in a way that the specific identity of the patient cannot be determined. If the patient protests at having her story chronicled in agonizing detail to the public, could the good doctor respond that because the information is not identifiable to the specific patient, even with additional research, it is not "personal information." And, because it is not personal information, the patient lacks any privacy claim? To my mind, this reasoning fails to account for the residual privacy interest that exists, notwithstanding the anonymity.

Jerry Kang, *Cyberspace Privacy*, 50 Stan. L. Rev. 1193, 1209 (1998). *See also* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 11 U. Chi. Legal F. 139, 149-51 (1996) (discussing how context can sometimes provide identity information of facially anonymous e-mails).

Similarly, there are important and distinct privacy interests to be considered in this case involving the transfer of "de-identified" personal

information. The information may, in practice, be re-identified. Even if it is not, the data may still impact a cognizable private interest. As one legal scholar puts it, "data can either be useful or perfectly anonymous, but never both." Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* 4 (University of Colorado Law Legal Studies Research Paper No. 09-12, 2009).[3]

III. IMS Health's "De-identification" Practices Do Not Obviate the Medical Privacy Interests of Vermont Residents.

Appellants IMS Health Inc. and Verispan, LLC are data-mining companies that purchase and compile prescription information in order to sell the data to private companies and law enforcement agencies, as well as research and academic institutions. Their biggest clients by far are pharmaceutical companies, which use the data extensively for "detailing," targeting doctors for office visits by sales representatives.

The patient data collected by IMS Health is not secure. Quasi-identifiers can be used for re-identification because they can be linked to external databases that contain identifying variables. This method, record linkage, occurs when two or more databases are joined. Such

[3] *Available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

information can be obtained through public records, such as birth and death certificates. *See* Salvador Ochoa et al., *Re-identification of Individuals in Chicago's Homicide Database: A Technical and Legal Study*, Massachusetts Institute of Technology (2001) (utilizing the Social Security Death Index and de-identified information about Chicago homicide victims, the researchers were able to re-identify 35% of the victims). Using record linkage, de-identified data can also be easily re-identified. For example, by utilizing date of birth, gender, and zip code information for members of the public, a researcher was able to uniquely identify 87% of the US population. Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality* at 98-99. Even Google, one of the leaders in information collection and disclosure on the internet, has admitted, "[it] is difficult to guarantee complete anonymization[.]" Chris Soghoian, *Debunking Google's Log Anonymization Propaganda*, Surveillance State Blog, Sept. 11, 2008.[4]

It is easier to identify people who have a unique combination of quasi-identifiers compared to others in the population. For example, the sole female in a male-dominated working group creates population

[4] *Available at* http://news.cnet.com/8301-13739_3-10038963-46.html.

uniqueness. Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality* at 98-99. Similarly, when a person has unique quasi-identifiers compared with the rest of the individuals in the sample group, that person's sample is unique. This also makes the person easier to identify because the unique feature makes the person easier to trace in the real world. This can often be done without name, Social Security number, address, phone number, or other easily identifiable data.

Re-identification of data through record linkage creates additional problems for public figures about whom more personally identifiable information is commonly known. For example, a former governor of Massachusetts had his full medical record re-identified after a researcher cross-referenced public Census information with de-identified health data. Latanya Sweeney, *Roundtable Discussion: Identifiability of Data, Subcomm. on Privacy and Confidentiality*, Nat'l Comm. on Vital and Health Statistics, Jan. 28, 1998.[5] Twelve percent of a population of voters can be re-identified base date birth date alone. With birth date and gender, that number increases to 29%, with birth

[5] *Available at* ttp://npalliance.org/images/uploads/IssueBrief-Prescribing_Data_low_res.pdf.

date and zip code it increases to 69%, and with full postal code and birth date, 97% of people can be re-identified. *See* Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*. Even information as seemingly innocuous, such as movie ratings, can be used to re-identify data. Researchers from the University of Texas found that if an adversary knows six precise ratings a person in the Netflix database has assigned to obscure movies, without any other information, the adversary can identify that person 84% of the time. Arvind Narayanan and Vitaly Shmatikov, *Robust De-anonymization of Large Datasets (How to Break the Anonymization of the Netflix Prize Dataset)* 12, Feb. 5, 2008. If the element of time is added, i.e. if the adversary knows when the ratings were assigned, to six movies (obscure or non-obscure), he can identify 99% of the people in the Netflix database. *Id.* This raises a particularly significant threat, because "researchers have found data fingerprints in pools of non-PII data, with much greater ease than most would have predicted[, suggesting] that maybe everything is PII, to one who has access to the right outside information." Ohm, *Broken Promises of Privacy* at 21. The ease with which records can be linked for re-identification purposes also creates

unique problems for victims of harassment or domestic violence. This is especially true because the abusers may have additional information that could lead to greater ease of re-identification. For example, many abusers know of victims' past illnesses and the time frame of their occurrence.

The district court's opinion in this case notes that IMS Health "manipulate[s]" patient data, but that the manipulated data still shows "physicians' prescribing patterns in terms of gross number of prescriptions and inclination to prescribe a particular drug." IMS Health v. Sorrell, ___ F. Supp. 2d ___, No. 1:07–CV–188 (D. Vt. Apr. 23, 2009). However, no statute defines how IMS Health must de-identify data. Nor is IMS Health legally required to de-identify. The closest governing regulation, the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191., requires the removal of 18 specific identifiers that relate to patient identity, including geographic subdivisions smaller than a state, all elements of date (except year), biometric identifiers, Social Security and medical record numbers. 45 C.F.R. § 164.514(b)(2) (2006). However, HIPAA does not cover pharmaceutical data-mining companies such as

IMS Health and Verispan. *See* 45 C.F.R. § 160.103 (2006). Further, the ease with which data can be re-identified renders the HIPAA protections "illusory and underinclusive, because it deregulates the dissemination of certain types of data that can still be used to reidentify and harm." Ohm, *Broken Promises of Privacy* at 34.

Although de-identification measures are increasingly innovative and computationally complex, patient data is still vulnerable to attacks because sophisticated re-identification programs are also being developed. Individuals can be re-identified using information such as zip code, date of birth, and gender and then comparing that data to publicly available information. Such information is easily accessible via birth and death records, incarceration reports, voter registration files, and driver's licensing information. Khaled El Emam et al., *Evaluating Common De-identification Heuristics for Personal Health Information*, 8 J. Med. Internet Res. 4 (2006). As University of Colorado Law School professor Paul Ohm notes, "no matter how effectively you follow the latest reidentification research, folding newly identified data fields into your laws and regulations, reidentification researchers will always find another data field type you do not yet cover." Ohm, *Broken Promises of*

Privacy at 35.

Data re-identification has broad implications. It can be used for business purposes, as well as by individual citizens employing widely available tools. Re-identification can also be used for many types of investigative reporting, especially investigations involving celebrities or politicians. Ochoa, *Re-identification of Individuals in Chicago's Homicide Database: A Technical and Legal Study; cf.* Barron H. Lerner, When Illness Goes Public 144 (2006) (detailing Steve McQueen's use of a pseudonym while receiving mesothelioma treatment at Cedars-Sinai Medical Center in 1980). The information gleaned from health records could provide sensitive and potentially embarrassing reports. It can also be used by someone trying to identify a very small group of individuals with a similar characteristic. Re-identified data may also be useful in divorce proceedings or by perpetrators of crime who may have specific information on one particular individual that they can then use to identify that person's health records.

An additional privacy interest is implicated through pharmaceutical data-mining. Increasing the role companies have in determining patient treatment through personalized medicine opens

the door to more intrusive use of patient information. This leads to situations where patients have less control over their personal treatment plans. With personalized medicine, pharmaceuticals and other treatments are specifically tailored to a patient's genetic profile. Gary E. Merchant, *Personalized Medicine and the Law*, 44 *Arizona Attorney* 12 *(*2007*)*. One of the most significant impediments to the implementation of personalized medicine is the "real and perceived risk of genetic discrimination and privacy violations." *Id.* at 19. Many patients are hesitant to partake in existing genetic tests for fear that third parties, including employers or insurers, could use the information collected against them. *Id.* This underscores the need to ensure that the patient privacy interest in matters involving the transfer of sensitive prescribing information is given sufficient weight.

CONCLUSION

Amicus Curiae respectfully requests this Court to grant Appellee's motion to affirm the decision of the lower court.

Respectfully submitted,

MARC ROTENBERG
Application for admission pending
JOHN A. VERDI
JARED KAPROVE
(VA. ADMISSION PENDING)
KIM NGUYEN
(MD. ADMISSION PENDING)
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

September 15, 2009

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(B)(i). This brief contains 3,301 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word 2007 in 14 point Century Schoolbook style.

Dated: September 15, 2009

MARC ROTENBERG
Application for admission pending
JOHN A. VERDI
JARED KAPROVE
(VA. ADMISSION PENDING)
KIM NGUYEN
(MD. ADMISSION PENDING)
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

ANTI-VIRUS CERTIFICATION

In the matter of *IMS Health Inc. v. Sorrell*, Docket No. 09-1913-cv (L), I, Marc Rotenberg, certify that I used Symantec Anti-Virus 9.0.1.1000, Scan Engine Version 91.2.0.30; Virus Definitions Version 9.14.2009 Rev. 3 to scan for viruses the PDF version of the Brief of Appellees that was submitted in this case as an email attachment to <briefs@ca2.uscourts.gov> and that no viruses were detected.

Dated: September 15, 2009

MARC ROTENBERG
Application for admission pending
JOHN A. VERDI
JARED KAPROVE
(VA. ADMISSION PENDING)
KIM NGUYEN
(MD. ADMISSION PENDING)
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on this 15th day of September, 2009, ten copies of the foregoing Brief of *Amicus Curiae* were filed with the Clerk of the Court by overnight delivery service, and two copies were shipped by commercial carrier for next-delivery upon the following::

Thomas R. Julin, Esq.
Jamie Isani Zysk, Esq.
Patricia Acosta, Esq.
Hunton & Williams LLP
1111 Brickell Avenue, Suite 2500
Miami, FL 33131

Robert N. Weiner, Esq.
Jeffrey L. Handwerker, Esq.
Sarah Brackney Arni
Arnold & Porter LLP
555 Twelfth Street, N.W.
Washington, D.C. 20004-1206

Bridget C. Asay, Esq.
Assistant Attorney General
Office of the Attorney General
109 State Street
Montpelier, VT 05609-1001

Dated: September 15, 2009

_____

MARC ROTENBERG
Application for admission pending
JOHN A. VERDI
JARED KAPROVE
(VA. ADMISSION PENDING)
KIM NGUYEN
(MD. ADMISSION PENDING)
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-114