KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

# MEMO ON *SORRELL V. IMS HEALTH INC.*
## Supreme Court Case Requires Nuanced Understanding of Privacy

**March 22, 2011**

A case pending before the U.S. Supreme Court has the potential to do real damage to privacy protections, but understanding the various risks posed by the case requires some careful unpacking of the ways in which "privacy" is – and is not – at issue. In this paper, we focus on two aspects of the case: First, we explain why it is very important to recognize the valid distinctions between personally identifiable data and "de-identified" data. We explain that privacy could actually be harmed if the Court were to accept the claims, made in some briefs in the case, that there is no difference between identified and de-identified data. Second, we examine the claim that doctors have a "privacy" right in their drug prescribing practices. We explain that, while the patient-doctor relationship is based on confidentiality and the trust it generates, it is not useful – and would undermine other health care goals – to speak of doctors as having a "privacy" right in their drug prescribing practices.

## Can Vermont Prohibit Drug Companies from Using Patient De-identified Data to Market Drugs to Doctors?

The case is *Sorrell et al. v. IMS Health Inc. et. al.*[1] The U.S. Supreme Court is scheduled to hear arguments on April 26. At issue is a Vermont state statute that prohibits drug companies from using certain data to market drugs to doctors and others who prescribe drugs. The information at issue is lists, largely obtained from pharmacies and pharmacy benefit managers, showing what drugs each doctor has been prescribing. Sales reps for drug companies use this information for a range of purposes, including trying to convince the doctor to prescribe more of their company's drugs and to prescribe more brand name drugs instead of generics.[2]

Vermont legislators wanted to control the costs associated with increased prescribing of more expensive, brand-name drugs, and they wanted to address safety issues related to increasing off-label uses.[3] So they adopted a law saying that drug companies cannot obtain data about doctor's prescribing habits and use it to market drugs to prescribers unless the prescribers have consented.[4]

---

[1] Docket No. 10-779, scheduled for oral argument on April 26, 2011. http://www.scotusblog.com/case-files/cases/sorrell-v-ims-health-inc?wpmp_switcher=desktop.

[2] See Brief for Petitioner William H. Sorrell, as Attorney General of the State of Vermont, pages 7-10; http://www.americanbar.org/content/dam/aba/publishing/previewbriefs/Other_Brief_Updates/10-779_Petitioner.authcheckdam.pdf (hereinafter, Vermont Brief)

[3] Id. at pages 10-15.

[4] Id., describing Vermont Statutes title 18, section 4631.

The first thing to recognize about the data at issue is that it contains doctors' names but it does not contain patient names. The data is "patient de-identified" pursuant to standards established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA already prohibits the use of patient-identified data for marketing to patients or to doctors.[5] Vermont went one step further and said that even patient de-identified data cannot be used to market drugs to doctors.

Companies who compile the data – IMS Health Inc., Verispan, LLC, and Source Healthcare Analytics, Inc. – claim that their use of this data for marketing purposes is protected by the First Amendment.[6] Vermont (and the U.S. Solicitor General) argue that the statute is a reasonable exercise of the state's authority to regulate a commercial activity for the legitimate state goals of controlling drug costs paid by the state and preventing potentially dangerous off-label uses.[7] However, Vermont also argues that the statute was enacted to protect patient and prescriber privacy.[8] Amicus briefs filed by the medical community and some privacy advocates also assert that patient and prescriber privacy interests are at stake.[9] Thus the case sets up a dangerous conflict between privacy and the First Amendment. As amici argue, it would be a disaster if the Court were to hold that the First Amendment rights of corporations could trump the privacy interests of patients and others.[10] CDT shares these significant concerns. The entire fabric of American privacy law could be upset by such a ruling.

But are the defenders of the law properly invoking privacy in the first place? Certainly, medical data is sensitive, and, as explained in more detail below, CDT has been a leader in pointing out the risks associated with even de-identified data. But some of the privacy claims in the case are, in our estimation, seriously overbroad. Worse, if the Supreme Court were to accept some of the privacy claims, it could do damage to privacy by discouraging use of de-identified data. And claims that doctors have a privacy right in their drug prescribing practices could upset a host of policy goals associated with improving the efficiency and safety of the health care system.

## CDT's History on the Issue of HIPAA De-identified Data

CDT has a long history of promoting consumer privacy on the Internet, and our Health Privacy Project plays a leading role in promoting health privacy protections as the nation moves rapidly to electronic health records. We have testified before Congress on health privacy issues four

---

[5] See 42 U.S.C. Section 17935(d).

[6] Brief of Respondents IMS Health Inc. et al., http://sblog.s3.amazonaws.com/wp-content/uploads/2010/12/BIO-IMS.10-779.pdf. The Pharmaceutical Research and Manufacturers Association was a plaintiff in the case in the lower court and is expected to appear separately as a respondent in the Supreme Court case. Id. at page ii.

[7] Vermont Brief, beginning on page 20; Brief of the United States as Amicus Curiae Supporting Petitioners (hereinafter Brief of the Solicitor General), beginning on page 12, http://sblog.s3.amazonaws.com/wp-content/uploads/2011/03/10-779tsacUnitedStates.pdf.

[8] See Vermont Brief.

[9] See, for example, briefs of AARP, the Vermont Medical Society, and the Electronic Privacy Information Center (EPIC). http://www.scotusblog.com/case-files/cases/sorrell-v-ims-health-inc?wpmp_switcher=desktop.

[10] See, for example, briefs of the Electronic Frontier Foundation (EFF) and EPIC, http://www.scotusblog.com/case-files/cases/sorrell-v-ims-health-inc?wpmp_switcher=desktop; see also Brief of the Solicitor General, pages 33-35.

times in the last two-and-a-half years.[11] The Director of CDT's Health Privacy Project, Deven McGraw, was appointed by HHS Secretary Kathleen Sebelius in 2009 to serve a three-year term on the Health IT Policy Committee, a federal advisory committee created by Congress to advise the HHS Office of the National Coordinator for Health IT on health information privacy and security policy.

Moreover, CDT has long had an interest in policies governing the use of de-identified health data. The issues surrounding de-identified data are very important because there are many beneficial uses for health data that go beyond the direct treatment of patients. These other uses include public health monitoring, quality and effectiveness assessments, cost control, and research. If these secondary purposes can be served with de-identified data, that is far better for privacy, for it reduces the flow of identifiable data.

CDT held a workshop in September of 2008 on de-identification of health data, which brought together experts on data security and privacy. The workshop led to the development of a set of recommendations on de-identified data intended to strengthen protections for patient data while still ensuring its availability for a broad range of important purposes.[12] Overall, CDT concluded that de-identified data policies needed to be strengthened; of critical importance is the need to establish strict accountability for inappropriate re-identification. At the same time, we also argued that making data available in more anonymous forms for secondary purposes helps to promote information-rich health care and population health while protecting individual patient privacy.[13] Public policy is needed to both encourage less use of identifiable data and establish safeguards against re-identification of de-identified data.

## What is HIPAA De-Identification?

Under HIPAA, health data that is identifiable – data that contains patient names, addresses, and dates of services, for example – is "protected health information" and is subject to restrictions on access, use and disclosure. Data stripped of identifiers, which is useful for a number of important purposes, is exempt in whole or in part from regulation. Specifically, data is considered "de-identified" if it has been so stripped of identifiers that there is "no reasonable basis to believe" that the information can be used to identify an individual.[14] Data can be de-identified using one of two methods. The first method is statistical de-identification, where a qualified statistician determines that "the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information."[15] The second is the safe harbor method, which requires the removal of 18 specific types of identifiers.[16] Under either method,

---

[11] See http://www.cdt.org/testimony/testimony-deven-mcgraw-2; http://www.cdt.org/testimony/testimony-deven-mcgraw-1; http://www.cdt.org/testimony/testimony-deven-mcgraw-0; http://www.cdt.org/testimony/testimony-deven-mcgraw-standards-health-it-meaningful-use-and-beyond.

[12] "Encouraging the Use of, and Rethinking Protections for, De-Identified (and "Anonymized") Health Data," CDT, June 2009, http://www.cdt.org/paper/encouraging-use-and-rethinking-protections-de-identified-and-anonymized-health-data (hereinafter, CDT Paper on De-Identification).

[13] Id.

[14] 45 CFR Section 164.514(a).

[15] 45 CFR Section 164.514(b)(1)(i)-(ii).

[16] 45 CFR Section 164.514(b)(2)(i)-(ii).

once data meets the standard for de-identification, it is no longer subject to regulation under HIPAA.[17]

CDT does not believe that there are zero privacy interests in de-identified data. Among other things, there is a concern that data insufficiently de-identified could be re-identified. CDT believes that current HIPAA de-identification methods – in particular the safe harbor approach – are not as robust as they need to be to justify a "hands-off" approach to regulation. Consequently, CDT has recommended re-evaluating and updating de-identification standards to accommodate a rapidly changing data environment that makes it easier to re-identify.[18] We have also called on policymakers to enact strict prohibitions against inappropriate re-identification.[19] Moreover, in some contexts, such as online behavioral advertising, even de-identified data poses major concerns.[20]

However, CDT believes it is important that HIPAA and other health privacy laws maintain a distinction between fully identifiable data and data that has been properly de-identified – i.e., sufficiently striped of identifiers that there is no reasonable basis to believe the information can be re-identified. If privacy laws do not recognize a distinction between de-identified and fully identified data, then there will be little or no incentive to de-identify data and learn to work with it or to improve de-identification techniques. Instead, there will be a tendency to use fully identified data for secondary purposes such as public health and quality control, which would raise far greater privacy risk for individuals.

The American Recovery and Reinvestment Act of 2009 requires the Department of Health and Human Services to issue a report on the HIPAA de-identification standard,[21] and the HHS Office of Civil Rights, which oversees HIPAA, held two days of meetings on de-identification in March 2010.[22] Unfortunately, the report has yet to be issued. As a result, questions continue to linger about the protective value of HIPAA de-identification, while uses of this data appear to be proliferating at a rapid rate. Actual uses of de-identified data are difficult to quantify, as there are no requirements to track or report on its collection and use.[23] This lack of transparency increases suspicions about whether all such data use and disclosure is appropriate and not linked to identifiable individuals.

These are some of the nuances largely ignored in the briefs in the Supreme Court, which is why we are worried that an overbroad ruling could damage privacy by discouraging the use of de-identified data.

---

[17] HIPAA sets standards for "protected health information," 45 CFR Section 164.502(a), which is identifiable health information defined at 45 CFR 160.103. See also CDT Paper on De-Identification.

[18] CDT Paper on De-Identification.

[19] Id.

[20] See "Online Behavioral Advertising: Industry's Current Self-Regulatory Framework is Necessary, But Still Insufficient On Its Own to Protect Consumers," CDT, December 2009, http://www.cdt.org/report/online-behavioral-advertising-industrys-current-self-regulatory-framework-necessary-still-ins (we note, however, that there are no standards similar to HIPAA de-identification for "anonymizing" data in the online behavioral advertising context; most on-line behavioral advertisers are not covered by HIPAA).

[21] 42 USC 17954(c).

[22] http://edocket.access.gpo.gov/2010/2010-3663.htm.

[23] See CDT Paper on De-Identification.

We do note that some amici have raised questions about whether the particular hashing de-identification technique used by one or more of the respondent companies actually satisfies the HIPAA de-identification standard requiring a very low risk of re-identification.[24] This is a factual question that is not something the Supreme Court can sort out. Instead, HHS should explore whether this particular technique, used alone or in combination with other safeguards, is sufficient to meet the actual HIPAA de-identification standard. If in fact the data is readily susceptible to re-identification, the data doesn't meet the HIPAA standard. In such a case, a legal remedy to prevent the sale of this identifiable health information already exists in federal law and should be pursued.

## Do Prescribers Have a Privacy Interest in their Prescribing Behaviors?

Vermont and a number of amici have asserted that the state's interest in protecting prescriber privacy motivated the enactment of the statute.[25]

CDT has long recognized that the doctor-patient relationship is the foundation for building and maintaining public trust in the electronic collection and exchange of health information to improve individual and population health. However, we are concerned about claims by some amici of a privacy interest on the part of prescribers. The behavior of physicians and other health care professionals is routinely scrutinized by federal and state regulators, accrediting organizations, licensing boards, and health care plans, among others. A broadly recognized privacy interest in prescriber-identifiable data could have implications for multiple important issues, including quality measurement and public reporting, as well as comparative effectiveness research, which are critical to reform of our health care system. If the Court were to agree that prescriber records need to be protected like corporate "trade secrets"[26] or that there is no role for outside review of physician decision making, important reform activities that depend on access to and use of prescriber identified data could be impaired or prohibited. Doctors' frustration with having their treatment decisions second-guessed should not be addressed by inventing a right of prescriber privacy.

## Conclusion

So in many ways, *Sorrell v. IMS Health* is not about privacy in the way that defenders of the Vermont law claim. Yet a broad ruling by the court on de-identified data could have negative impact on patient privacy. And a broad statement by the Court on doctor "privacy" could derail other very timely initiatives. This is not the case, nor is the Supreme Court the institution, to make policy on either set of issues; the parties have offered other viable rationale for the Court to use to decide this case. There needs to be a policy conversation about the viability of the current de-identification standard, but this case needs to preserve the concept that there is a meaningful distinction between identified and de-identified data. It is up to other processes to ensure a continually robust de-identification standard and strict accountability for re-identification.

---

[24] See the briefs of EPIC and EFF, http://www.scotusblog.com/case-files/cases/sorrell-v-ims-health-inc?wpmp_switcher=desktop.

[25] See for example the briefs of the Vermont Medical Society, the New England Journal of Medicine et al., and AARP, http://www.scotusblog.com/case-files/cases/sorrell-v-ims-health-inc?wpmp_switcher=desktop.

[26] See brief of the New England Journal of Medicine at 11-13, http://www.scotusblog.com/case-files/cases/sorrell-v-ims-health-inc?wpmp_switcher=desktop.