5-1-2013

Pharmaceutical Company Data Mining in the Aftermath of Sorrell v. IMS Health: The Need for Comprehensive Federal Legislation to Protect Patient Privacy

Melody Rene Hsiou

PHARMACEUTICAL COMPANY DATA MINING IN THE AFTERMATH OF *SORRELL V. IMS HEALTH*: THE NEED FOR COMPREHENSIVE FEDERAL LEGISLATION TO PROTECT PATIENT PRIVACY

Melody R. Hsiou

INTRODUCTION

Pharmaceutical companies and drug manufacturers have long used the practice of data mining to increase sales and compete with generic drug makers. [1] Under law, pharmacies have the duty to track prescriber specific data when physicians prescribe medications to their patients.[2] Unbeknownst to most of the public and even prescribers, pharmacies then sell these raw data to data mining companies that compile, analyze, and format the information to sell to pharmaceutical companies.[3] This data, which reveals the prescribing habits of physicians, has proven to be highly valuable commodity that allows pharmaceutical companies to tailor sales presentations to doctors in an effort to increase sales.[4] However, this practice raises many concerns about patient privacy and threatens the safety and integrity of sensitive health information.

In response to these concerns and to stem rising health care costs, Vermont enacted the Vermont Prescription Confidentiality Law in 2007.[5] Vermont's law broadly banned the use, sale or transmission of prescriber-identifiable data without first obtaining the prescriber's consent. Several data mining companies, including, IMS Health, Source Healthcare Analytics, Inc., as well as PhRMA, brought suit, alleging that the statute impermissibly infringed upon their

---

[1] Isabelle Bibet-Kalinyak, *A Critical Analysis of Sorrell v. Ims Health, Inc.: Pandora's Box at Best*, 67 FOOD & DRUG L.J. 191 (2012).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] The Confidentiality of Prescription Information Act is also known as "Act 80;"*Sorrell*, 131 S.Ct. at 2660 ; The Vermont Prescription confidentiality Law, 2007 Vt. Acts and Resolves No. 80, §17 (2007).

freedom of speech under the First Amendment.[6] In November 2010, the Court of Appeals for the Second Circuit issued its ruling that Vermont's drug-marketing restrictions were unconstitutional. [7] The Second Circuit then overturned the statute, holding that it was unconstitutional for Vermont to restrict speech by data miners and pharmaceutical companies without demonstrating a compelling state interest to do so.[8]

In June 2011, the Supreme Court likewise struck down the Vermont law in *Sorrell v. IMS Health Inc*. (*Sorrell*), on the grounds that it was a First Amendment violation to restrict pharmaceutical marketers' access to and use of prescription data for advertising purposes.[9] The decision in *Sorrell* has affected how state governments can regulate the data mining industry.[10] This article will discuss the scope of *Sorrell* and its implications for data mining and patient privacy, suggest that pharmaceutical data mining should be regulated based on personal privacy concerns rather than commercial speech issues, and recommend that a patient-centered federal statute is needed to protect patient privacy.

Part I will provide background of data mining practices and how the pharmaceutical industry uses aggregated prescription data to increase profits through targeted advertising and marketing. Part II will discuss data mining's implications for medical privacy and confidentiality. Part III will describe existing state and federal efforts to protect patient privacy and describe cases that have been brought forth to challenge privacy laws. Part IV will argue that existing privacy protections are not adequate, particularly in regard to protecting de-identified health data, and discuss legal cases that illustrate these loopholes. Part V will argue that a comprehensive

---

[6] Sorrell v. IMS Health, 131 S.Ct 2653, 2672, 180 L.Ed.2d 544 (2011).
[7] Sorrell v. IMS Health, Inc., 131 S. Ct. 857 (2010).
[8] *Sorrell*, 180 L.Ed. 2d at 544.
[9] *Sorrell*, 131 S.Ct at 2653.
[10] Agatha M. Cole, *Internet Advertising After Sorrell v. IMS Health: A Discussion on Data Privacy & The First Amendment*. 30 CARDOZO ARTS & ENT. L.J. 283 (2012).

federal statute that protects patient privacy is needed, and lay out a recommended statute that is centered on patient, rather than prescriber, privacy.

Finally, this Note concludes that although *Sorrell* invalidates existing state prescription privacy laws, it leaves room for the creation of a much needed patient-centered federal statute that protects patient privacy.

I. PHARMACEUTICAL COMPANY DATA MINING

The health care industry has been pushed in new information-technology driven directions. The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, accelerates the goals of promoting the adoption of electronic health records (EHRs) and health information technology (HIT) tools to save costs and improve efficiency throughout the health care industry.[11] A major component of HITECH is the promotion of "meaningful use" of EHR systems through financial incentives payable by federal healthcare programs.[12] The meaningful use requirements, which include capturing clinical data, reporting quality measures, and using automated clinical decision support tools, have engendered the rapid growth of electronic health records. [13] The production of vast quantities of electronically encoded health data raises many concerns for potential HIT misuse.[14]

The safety and integrity of electronic health records are primarily governed by the Privacy and Security Rules of the Health Insurance Portability and Accessibility Act of 1996 (HIPAA).[15] HITECH aims to strengthen HIPAA's privacy rules by significantly increasing penalties and

---

[11] John Hazewinkel, *Digital Health Care Reform Under the HITECH Act*, MICH. B.J. 33, 2011.
[12] *Id.*
[13] *Id.*
[14] Erik Pupo, *Privacy and Security Concerns in Data Mining, Cinical Informatics Insights* (April 2012), http://www.himss.org/CI_Insights/HIMSSClinicalInformaticsInsights.asp?date=20100412.
[15] Hazewinkel, *supra* note 11 at 35.

reporting requirements.[16] However, despite these efforts to protect electronic health data, the "secondary use" of data still remains largely out of the realm of HIPAA's scope. [17] Secondary use of data refers to everything from the business use of communicating data for payment of health services, to other activities such as public health reporting, biomedical research, and sales marketing. [18] EHRs have largely streamlined the process of extracting information from raw data by structuring data in discreet, common formats that can create longitudinal profiles on patients.[19] This technique has contributed to the pervasive use of data mining.

"Data mining" is a term that describes the process of identifying significant or interesting data patterns that may be useful in decision making.[20] Data mining has the potential to improve management of data, increase business efficiencies, and support efficient delivery of care. Through data mining, raw data can be interpreted and used for knowledge discovery in outcomes research, epidemiology, drug and genome discovery, and biomedical research.[21] Data mining also has the potential to reveal unusual data patterns which might help detect disease outbreaks or expose healthcare fraud and abuse.[22] Data mining produces valuable data and may have many medical and public health benefits when used correctly and with patient protections.

However, data mining also has the potential for threatening medical privacy and confidentiality. This article will focus on pharmaceutical company data mining, which presents serious invasions of physician and patient privacy. Pharmaceutical data mining is the business of collecting information relating to prescribers' prescribing habits and then selling them to data

---

[16] Hazewinkel, *supra* note 11 at 35.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] Michael Heesters, *An Assault on the Business of Pharmaceutical Data Mining*, 11 U. PA. J. BUS. L. 789 (2009).
[21] *Id.*
[22] *Id.*

mining companies, which then sell detailed reports on prescribing patterns to pharmaceutical companies.[23] Pharmaceutical companies buy this valuable information to allow them to better target their sales force, allowing them to increase their marketing efficiency and greatly increase their profits.[24]

The protection of private health information is a major concern in the U.S. that has been acknowledged by several state and federal privacy laws.[25] On its face, the buying and selling of personal health information for pecuniary gain seems to violate prescriber and patient privacy rights. Indeed, data mining companies have admitted that prescriber-identifiable medical records expose the intimate details of what doctors prescribe to their patients, potentially infringing on physician-patient confidentiality.[26] However, pharmaceutical companies purport to comply with existing privacy laws by using only "de-identified" data that cannot be traced back to individual patients. Unfortunately, the growth of mass data and electronic information makes de-identification of data a realistic threat that should be regarded as a major state interest.

II. DATA MINING AND IMPLICATIONS FOR THE PHYSICIAN-PATIENT RELATIONSHIP AND PATIENT PRIVACY

The collaboration of pharmacies, data miners, and pharmaceutical companies has created a wealth of private health data that can be converted for commercial purposes. Using detailed reports on prescribing habits of physicians, pharmaceutical sales representatives, or "detailers,"

---

[23] Heesters, *supra* note 20 at 790.
[24] *Id.*
[25] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (defining federal health privacy rights); 45 C.F.R. § 160.101, et seq; 45 C.F.R. § 164.102, et seq (HIPAA Privacy Rule); Genetic Information Nondiscrimination Act (GINA), Pub. L. No. 110-233, 122 Stat. 881 (2008) (protecting individual genetic information).
[26] Brief for Respondent Pharmaceutical Research and Manufacturers of America, On Petition for a Writ of Certiorari, at 4, *Sorrell v. IMS Health Inc.*, 131 S. Ct. 857 (Dec. 15, 2010) (No. 10-779).

leverage the data to strategically target leading prescribers and design their presentations to detract from competitors.[27] Brand name drug manufacturers such as those represented by PhRMA are required by patent law to market their brand name drugs to physicians and patients in a very limited window of exclusivity.[28] This time constraint, combined with fierce competition from generic drug companies, have turned pharmaceutical data mining and targeted advertising into an extremely lucrative business. [29]

A. Negative Consequences of Pharmaceutical Data Mining

Pharmaceutical company data mining has many undesirable consequences. First, it may interfere with physician's prescribing practices and taint the physician-patient relationship.[30] Data mining reports aggregate prescriber specific information to target doctors who prescribe large quantities of drugs for certain conditions, doctors who regularly prescribe drugs from competing companies, and doctors who may be identified as early adopters of drugs new to the market.[31] Detailers then tailor their in-person presentations to build and maintain brand loyalty and highlight the weaknesses of competing drugs. [32] On average, primary care physicians interact with at least twenty-eight detailers each week and average specialists see at least 14.[33] These sales representatives also give prescribers around $1 million worth of free drug samples a year, which are commonly distributed to patients at no charge to the doctor.[34] Through these incentives and regular in-person visits, detailers often form close personal relationships with

---

[27] Isabelle Bibet-Kalinyak, *A Critical Analysis of Sorrell v. Ims Health, Inc.: Pandora's Box at Best*, 67 FOOD & DRUG L.J. 191 (2012).
[28] *Id.*
[29] *Id.*
[30] Christopher R. Smith, *Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information*, VT. L. REV. 932 (2012).
[31] *Id.*
[32] David Orentlicher, *Prescription Data Mining and the Protection of Patient's Interests*. 38 J.L. MED & ETHICS 74 (2010).
[33] IMS Health Inc. v. Ayotte, 550 F. 3d 42, 47 (1st Cir. 2008).
[34] Smith, *supra* note 30 at 935.

physicians that create glaring conflicts of interest.[35] For example, brand loyalty may possibly predetermine a physician's choice of which drugs to prescribe when there are more effective or less expensive alternatives on the market. [36] The physicians' duty to prioritize the patients' best interests may be overshadowed by these secretive marketing techniques. [37]

Further, data mining and detailing drives up health care costs. Unlike generic drugs, brand name drugs have a high profit margin for manufacturers. [38] On average, brand name drug companies make an annual profit between 15% and 20%, placing their profit margins far above those in other industries.[39] The practices of detailing and data mining themselves are extremely costly but very profitable; in 2005, one data mining company made $1.75 billion in revenue just from selling prescriber data to brand name pharmaceutical companies.[40] The amount of money drug companies spend on detailing has more than doubled between 1998 and 2008, and pharmaceutical companies now spend more money marketing to prescriber than they do to marketing to consumers. [41]This aggressive marketing of brand name drugs leads to overprescribing of unnecessary or most costly drugs, resulting in greater costs to individuals, insurers, and federal health care programs.[42]

While several states have statutes aimed to restrict the sale or use of identifiable prescriber data for pharmaceutical companies' sales purposes, the Supreme Court in *Sorell* has largely

---

[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Amanda L. Connors, *Big Bad Pharma: an Ethical Analysis of Physician-Directed and Consumer-Directed Marketing Tactics*, 73 ALB. L. REV. 243, 247 (2009).
[40] *Id.*
[41] Sheila Campbell, *Promotional Spending for Prescription Drugs*, CONGRESSIONAL BUDGET OFFICE (Dec. 2, 2009), http://cbo.gov/ftpdocs/105xx/doc10522/12-02-DrugPromo_Brief.pdf.
[42] IMs Health Inc. v. Mills, 616 F. 3d 7, 17 (1st Cir. 2010).

invalidated them.[43] The Court based its decision on the theory that the statutes wrongfully infringed on the free speech of the pharmaceutical companies' sales representatives. [44] In doing so, the Court has essentially given data miners the First Amendment right to use and sell private health information without patients' consent.[45] The *Sorrell* Court's focus on commercial speech issues largely ignored a fundamental issue at hand, which is the violation of medical privacy laws.[46] Continuing to ignore these privacy interests will prove to be harmful as the use of electronic health records proliferates and data becomes increasingly vulnerable.

B. The Importance of Protecting Patient Prescription PHI

The use and sale of personal health information (PHI) for commercial purposes should be considered an intrusion of patient privacy that necessitates greater protections. In 2010, Americans filled 3,703,594.389 prescriptions.[47] Every one of those prescriptions discloses PHI such as the patient's name, age, gender, address, the date and location the prescription was filled, the identity of the prescribing physician, and the identity and dosage of the drug prescribed.[48] Prescription profiles could make it difficult for Americans who lack insurance to acquire coverage.[49]Many consumers and insurance agents are not aware that large insurance companies have access to applicants' prescription histories.[50] The prescription data, which includes possible medical conditions and a numerical score predicting how much a person will cost an insurer, is

---

[43] *Sorrell,* 131 S.Ct at 2653.
[44] *Id.*
[45] Brief for Respondent Pharmaceutical Research and Manufacturers of America, On Petition for a Writ of Certiorari, at 4, *Sorrell v. IMS Health Inc*., 131 S. Ct. 857 (Dec. 15, 2010) (No. 10-779).
[46] *Id.*
[47] Smith, *supra* note 30 at 932.
[48] Smith, *supra* note 30 at 932.
[49] Chad Terhune, *They Know what's in Your Medicine Cabinet*, Businessweek Magazine (July 22, 2008), www.businessweek.com/stories/2008-07-22/they-know-what's-in-your-medicine-cabinet,.
[50] *Id.*

available in the form of online reports and cost only about $15 per search.[51] In 2007, the Federal Trade Commission (FTC) conducted an investigation on two companies that prepared these prescription reports: MedPoint and IntelliScript.[52] Companies like Medpoint and IntelliScript purchase the data they disseminate mainly from pharmacy-benefit manager (PBM) companies that provide services to insurers and employees[53]. In that capacity, the PBMS are able to broadly access prescription information from drugstores. According to the FTC, there are no privacy laws or regulations to prevent PBMs from gathering this data.[54]

The FTC investigation found that these two companies violated federal law because their system was hidden from consumers.[55] However, the FTC imposed no penalties and now merely requires disclosure if prescription information causes denial of coverage or other adverse actions.[56] Furthermore, patients are not notified if the initial profile disclosure leads to requests for more medical information that result in subsequent denial.[57] Privacy advocates have questioned how insurance carriers can ensure that they are obtaining accurate prescription histories, especially with people with very common names.[58] Further, there is also the concern that widespread and legitimate off-label use of prescription drugs, such as the use of antidepressants as a sleep aid, may cause unfair prejudice towards patients.[59]

In accordance with federal health privacy standards in HIPAA, PHI must be "de-identified" or encrypted prior to being distilled and aggregated for prescription data reports. In order to meet HIPAA standards, data must be sufficiently de-identified by removing certain factors such as

---

[51] Terhune, *supra* note 49.
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*

name, age, and social security number so that it "cannot be linked to personal data by third parties receiving the anonymous information."[60] HIPAA allows for two methods of de-identification: a statistical determination that the level of de-identification makes re-identification unlikely, or the removal of a specific set of identifiers (the "safe harbor" method). [61] Once data is de-identified, it is free from regulation under HIPAA. Unfortunately, especially with the safe harbor method, there is evidence that certain information can be included in de-identified data that may be unique to particular patients.

Most patients may share the view that one data is de-identified, it cannot be traced back to them.[62] However, all data has a unique signature that prevents it from ever being truly identified.[63] This signature, in combination with the longitudinal nature of a patient's electronic health record and the growing amount of publicly available personal information on the internet, may allow data to be easily re-identified. Inadvertent data disclosures to secondary users such as insurance companies and managed care evaluators may lead to discriminatory and exclusionary treatment.[64]

The privacy interests in safeguarding these medical records is substantial and the "de-identification" techniques adopted by data-mining firms do not adequately protect patient privacy.[65] There are no uniform national standards that dictate the appropriate level of data

---

[60] Christine Porter, *De-Identified Data and Third Party Data Mining: The Risk of Re-identification of Personal Information*, 5 SHIDER J.L. COM. & TECH. 3, para. 8 (2008).
[61] National Institute of Health, *The HIPAA Privacy Rule* (Jan. 2004), http://privacyruleandresearch.nih.gov/research_repositories.asp.
[62] *Id.*
[63] Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers?*, 1 DREXEL L. REV. 216 (2009).
[64] Pupo, *supra* note 14.
[65] *see* Electronic Privacy Information Center, *IMS Health v. Sorrell* (Jun. 23, 2011), http://epic.org/privacy/ims_sorrell/.

stripping necessary to insure against re-identification.[66] To compound the problem, after the initial breach of individual patient privacy through re-identification, there are no rules governing additional and future re-identification. [67]

Further, even if prescription PHI remains de-identified or encrypted, patients may feel unease, embarrassment, or stress simply from knowing that their information is being disseminated and used without their consent.[68] Patients may be less likely to fill prescriptions for certain conditions, or they may be less likely to seek health care.

III. EXISTING PRIVACY PROTECTIONS

A. Nation's Interest in Protecting Medical Privacy: HIPAA Privacy and Security Rule and HITECH

The nation has recognized its interest in protecting patient PHI by enacting existing legal protections through HIPAA and the HITECH Act.[69] The Privacy Rule, which is promulgated pursuant to HIPAA, requires covered entities, defined as health plans, health care clearinghouses, and health care providers who transmit health information electronically, to comply with provisions governing the disclosure of protected health information.[70] The Privacy Rule permits limited uses and disclosures of protected health information, most notably disclosures for the purposes of treatment, payment, and health care operations. [71]

---

[66] Terry, *supra* note 63, at 3 n.9.
[67]Porter, *supra* note 60.
[68] Smith, *supra* note 30 at 932.
[69] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936; Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 115 (2011).
[70] Public Welfare Security and Privacy, 45 C.F.R. pts. 160, 164 (2010).
[71] 45 C.F.R. §164.502(a).

The HITECH act amended HIPAA by requiring covered entities to notify affected persons and HHS when unsecured PHI has been breached or subject to unauthorized disclosure.[72] HITECH further supplemented HIPAA by requiring business associates of covered entities to comply with HIPAA's privacy and security requirements.[73]

B. State Legislation Restricting the Release of Prescription Information

Several states have also recognized the need to protect patients' right to privacy of PHI within state constitutions and state privacy statutes.[74] However, state courts are greatly varied in the degree of protection they are willing to offer with regard to patient prescription PHI.[75] For purposes of this discussion, this section will describe the specific state legislative responses to data mining in detailing in New Hampshire, Vermont, and Maine. Since 2007, each of these three states has enacted statutes that aim to restrict the practice of data mining and using prescription information for marketing and detailing purposes.[76]

In 2006, New Hampshire enacted the Prescription Information Law (PIL), which prohibited the license, was the first state to create a statute with the goal of restricting data mining of prescription information. The law prohibited the license, transfer, use, or sale of patient-identifiable and prescriber-identifiable prescription information for certain commercial purposes such as advertising, marketing, or promotion.[77] This prohibition applied to "any activity that could be used to influence sales or market share of a pharmaceutical product, influence or

---

[72] 42 U.S.C. §17932 (2006).
[73] 42 U.S.C. §§17931, 17934.
[74] Smith, *supra* note 30 at 944; Catherine Louisa Glenn, *Protecting Health Information Privacy: The Case for Self-Regulation of Electronically Held Medical Records*, 52 VAND. L. REV. 1695, 1609, n.25 (2000) (identifying the protection of health information privacy in several states including Alaska, Arizona, California, and Florida).
[75] *Id.*
[76] Smith, *supra* note 30 at 944.
[77] N.H. Rev. Stat. Ann. § 318:47-f (2011).

evaluate the prescribing behavior of an individual health care professional, or evaluate the effectiveness of a professional pharmaceutical detailing sales force."[78]

Vermont enacted a similar law in 2007, stating that pharmaceutical manufacturers, marketers, electronic transmission intermediaries, pharmacies, and similar entities could not "sell, license, or exchange for value regulated records containing prescriber-identifiable information, nor permit the use of regulated records containing prescriber-identifiable information for marketing or promoting a prescription drug, unless the prescriber consents." The Vermont law allowed prescribers to opt-in, thereby agreeing to allow the use of their prescriber-identifiable data for marketing purposes.[79]

Finally, in 2008, Maine enacted an opt-out statute that allowed the use of prescriber data for marketing purposes unless the prescriber chose confidentiality protections.[80] As a part of licensing applications, Maine prescribers could opt to protect their identifying information that would be otherwise be used for marketing purposes by carriers, pharmacies, and prescription drug intermediaries.[81] If the prescriber opted out, carriers could not "license, use, sell, transfer or exchange for value, for any marketing purpose, prescription drug information that identifies directly or indirectly the individual."[82]

IV. EXISTING LAWS DO NOT ADEQUATELY PROTECT PATIENT PHI

A. State Prescription PHI Privacy Laws have been invalidated by Sorrell

Existing state statutes such as the ones in Vermont, New Hampshire, and Maine, have been largely invalidated by the *Sorrell* decision. However, even if these statutes were upheld as

[78] *Id.*
[79] Vt. Stat. Ann. tit. 18, § 4631(d) (West 2011).
[80] Me. Rev. Stat. Ann. tit. 22, § 1711-E (2011).
[81] *Id.* § 4-A.
[82] *Id.* § 2.

they were, they contained several statutory weaknesses and arguably did not go far enough to protect patient privacy. Namely, the statutes were targeted primarily at the data mining industry and sought to regulate detailing from the prescribers' perspective rather than the patients'.[83] This prescriber centered focus tends to create the notion that prescribers, not patients, are empowered to control the flow of confidential information. [84]

In addition, these statutes did not address protection of de-identified or encrypted patient prescription PHI. [85] Only the Maine statute, in its phrase "identifies directly or indirectly," can be read to contain language that encompasses de-identified or encrypted PHI. [86] However, the narrow application of restricting sales to only carriers and drug information intermediaries, and only for marketing purposes, left room for entities such as researchers or drug manufacturers to use prescription PHI for marketing and other purposes without violating the statute.[87] All three states prohibit the use of prescription for marketing purposes, but this narrow scope does not address the legitimate desires that patients may have to protect their information from activities other than marketing, such as in research studies.[88]

Another weak point of these statutes is that they fail to include clear compliance and enforcement provisions.[89] For example, the New Hampshire and Maine statutes both rely on data miners, insurers, and pharmacies to monitor their own customers to prevent the transfer of

[83] Smith, *supra* note 30 at 977.
[84] Me. Rev. Stat. Ann. tit. 22, § 1711-E-4-A (detailing Maine's opt-out approach); Vt. Stat. Ann. tit. 18, § 4631(c)(1) (detailing Vermont's opt-in approach).
[85] Smith, *supra* note 30 at 977.
[86] Me. Rev. Stat. Ann. tit. 22, §§ 1711-E-2, E-1-F (2011).
[87] IMS Health Inc. v. Mills, 616 F.3d 7, 33 (1st Cir. 2010) (Lipez, J., concurring).
[88] Smith, *supra* note 30 at 982.
[89] *Id.*

prescription information for marketing purposes.[90] In addition, the data-mining statutes are not sufficiently transparent to raise awareness of statutory violations.[91] None of the three statutes contain clear provisions for how prescribers and patients would become aware of information breaches or even become aware that their prescription information was being used to target them through marketing techniques.[92]

In *Sorrell*, data mining companies argued that physicians did not opt-into the privacy protection program and concluded that it was because they had no expectation of privacy. However, the program was not widely publicized and many physicians were not aware that they had the option. In some cases, physicians may not have even known that their prescribing habits were being documented and did not understand the breadth and sophistication of detailing practices. Although these statutes have been deemed unconstitutional, privacy concerns will continue to become less speculative and more realistic, and should qualify as substantial state interests that need to be addressed. [93]

B. Professional Ethics Based Patient Privacy Protections Have not been Effective

Three major professional and ethical codes have also been developed to address concerns stemming from data mining and detailing. The first code is the American Medical Association's (AMA) Prescription Data Restriction Program (PDRP), which aims to curtail the use of prescription PHI for marketing purposes.[94] The PDRP gives prescribers the option to opt-in to a data mining program that prohibits pharmaceutical companies from giving data to marketers for

---

[90] *Mills*, 616 F.3d at 40-41 (Lipez, J., concurring) (Under the Maine law, pharmacies and data miners must impose a contractual obligation on their customers not to use prescription information for marketing purposes).
[91] Smith, *supra* note 30 at 982.
[92] *Id.*
[93] Annie Macios, *Who's Watching What? — Data Mining Raises Privacy Issues*, Radiology Today (January 12, 2009), http://www.radiologytoday.net/archive/rt_011209p20.shtml.
[94] *See generally* Barry D. Alexander et al., *Fundamentals of Health Law* 20, 31, 77, 348-59, 483 (American Health Lawyers Association, 5th ed. 2011).

a period of three years, with an option to extend by the prescriber.[95] Similar to the weakness highlighted in the state statutes, the PDRP allows physicians instead of patients to restrict access to prescription information.[96]

PhRMA's professional code was also revised to demonstrate a commitment by PhRMA to examine its own marketing practices and limit those that may be deemed inappropriate.[97] However, PhRMA's code is inadequate in that it also only addresses uses of prescriber data.[98] Moreover, both the PDRP and PhRMA's code have weak enforcement provisions that rely on voluntary compliance of interested parties.[99]

The third ethical code is the American Pharmacists Association's (APhA) Code of Ethics for Pharmacists, which requires pharmacists to place "concern for the well-being of the patient at the center of professional practice" and to maintain privacy and confidentiality.[100] Although this is the only ethical code that specifically mentions patient privacy, it does not protect the confidentiality of PHI that has been disclosed by pharmacists to third parties such as pharmaceutical manufacturers.[101] Thus, after information has been transmitted from a pharmacy to a data miner or pharmaceutical manufacturer, the duty of confidentiality to no longer applies

---

[95] Alexander D. Baxter, *IMS Health v. Ayotte: A New Direction on Commercial Speech Cases*, 25 BERKELEY TECH. L.J. 649, 650 (2010)

[96] Orentlicher, *supra* note 32, at 78 (arguing the providers should not have sole authority for protecting the privacy interests of patients).

[97] Pharmaceutical Researchers and Manufacturers of America, *Code on Interactions with Healthcare Professionals 2* (2008), www.phrma.org/sites/default/files/108/phrma_marketing_code_2008.pd.

[98] *Id.* at 13; John R. Washlick & Sidney Summers Welch, *Physician-Vendor Marketing and Financial Relationships Under Attack*, 2 J. HEALTH & LIFE SCI. L. 151, 186 (2008) (outlining the 2008 revisions to PhRMA Code).

[99] Joshua Weiss, *Medical Marketing in the United States: A Prescription for Reform*, 79 GEO. WASH. L. REV. 260, 264 (2010) (arguing that the PhRMA Code's voluntary compliance provision invites noncompliance).

[100] American Pharmacists Association, *Code of Ethics for Pharmacists* (Feb. 19, 2012), http:// www.pharmacist.com/AM/Template.cfm?Section=Search1&template=/ CM/HTMLDisplay.cfm&ContentID=2903.

[101] Grace-Marie Mowery, *A Patient's Right of Privacy in Computerized Pharmacy Records*, 66 CIN. L. REV. 697, 718 (1998).

for information from the drug manufacturer to the patient.[102] Notably, the PhRMA Code applies only to pharmaceutical companies, leaving the data-collection industry completely unregulated.[103] Overall, the ethical codes regarding prescription PHI privacy do not place enough emphasis on protecting the patients' privacy interests and lack effective enforcement mechanisms.[104]

C. HIPAA: Loopholes Allow for "Authorized" Disclosures of PHI

HIPAA allows individuals to obtain a list of who has accessed their PHI from their covered entities.[105] However, a loophole in HIPAA law allowed covered entities and other healthcare providers to not report disclosures of PHI that pertained to health care operations.[106] HITECH contains mandatory enforcement penalties for "willful neglect" [107] and Congress expects there to be a stronger position taken on enforcement of protecting individuals' PHI. Under HITECH, communications are not considered related to health care operations if the covered entity receives a payment for making the communication.[108]However, a communication is no longer considered a healthcare operation that requires an individuals' authorization unless the communication: (1)describes only the drug that is currently prescribed and there is a reasonable amount of payment for the information; or (2) it is made by a covered entity or business associate that has been authorized by the individual to whom it is making the communication.[109] Therefore, it appears that pharmaceutical marketing practices, like the use of patient information

---

[102] Sharon R. Schawbel, *Are You Taking Any Prescription Medication?: A Case Comment on* Weld v. CVS Pharmacy, Inc., 35 NEW ENG. L. REV. 909, 945 (2001).
[103] Mowery, *supra* note 101, at 701.
[104] Smith, *supra* note 30 at 982.
[105] 45 C.F.R. §164.528.
[106] 45 C.F.R. §164.528.
[107] *See* 42 U.S.C. §1320d-5 (Section 1176 of the Social Security Act), as amended by Section 13410 of HITECH.
[108] *See* 42 U.S.C. §1320d-5 (Section 1176 of the Social Security Act), as amended by Section 13406(a)(2) of HITECH.
[109] 45 C.F.R. §164.501, as adjusted by section 13406(a)(2) of HITECH.

sold by pharmacies to send letters encouraging prescription switches, may be acceptable under HITECH.[110]

HIPAA does not offer strong privacy protections, if any, for de-identified prescription PHI. Pursuant to the Privacy Rule of HIPAA, a covered entity's use of prescription information that is deemed to be de-identified or encrypted is open to unrestricted dissemination. The Privacy Rule does not adequately protect de-identified PHI, stating that PHI is de-identified if "the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."[111] Further, the HIPAA Security Rule, which requires encryption to render prescription "unusable, unreadable, or indecipherable to unauthorized individuals," does not create solutions for situations in which encrypted data becomes unencrypted and viewed by unauthorized sources.[112] The Security Rule considers encrypted prescription PHI to be secured PHI, which creates a broad safe harbor for covered entities and business associates to avoid liability for the unauthorized disclosure of protected health information. [113]

In addition to the risk of re-identification and unencryption, privacy advocates fear that HIPAA's regulations do not go far enough to protect patient PHI, especially with the advent of coordinated care delivery systems.[114] For example, in 2007, the pharmacy chain CVS and the pharmacy benefits manager Caremark merged to create the corporate entity CVS Caremark. In a pending Texas lawsuit, *Muecke Co. v. CVS Caremark Corp*., plaintiffs allege that Caremark, the benefits manager side of the entity, collected identifiable prescription health information, even

---

[110] Leslie Restaino, *Data Protection in the Pharmaceutical Industry: Concerns and Considerations*, 5 INT'L. IN-HOUSE COUNS. J. 17 (2011).
[111] 45 C.F.R. §164.514 (b)(2)(ii).
[112] Robert D. Fram, Margaret Jane Radin & Thomas P. Brown, *Altered States, Electronic Commerce and Owning the Means of Value Exchange*, 1999 STAN. TECH. L. REV. 2, 15-16 (1999).
[113] 74 Fed. Reg. 19,006, 19,006-08 (Apr. 27, 2009)(to be codified at 45 C.F.R. pts. 160, 164).
[114] Smith, *supra* note 30 at 987.

for non-CVS prescriptions, and transferred that information to CVS pharmacies.[115] For the purpose of coordinating patients' drug benefits, Caremark would receive the patient's name, date of birth, gender, phone number, social security number, address, prescription history, and the prescriber and identity of the current prescription.[116] Caremark would then use a common information technology platform to share that information with the pharmacy side of CVS Caremark, and that information would then be sold to drug companies for directly marketing to patients who appeared to be likely candidates for a drug according to their prescription histories.[117] In addition, the complaint also states that CVS used patient information to "directly target non-CVS patients and solicit their business to CVS-owned retail stores and their purchase of CVS-branded products." [118]

In cases such as these, entities may skirt HIPAA regulations through creative corporate structuring that allow for broad sharing of patient PHI. As a single corporate entity under HIPAA, CVS Caremark could lawfully attain authorized access patient's prescription PHI and then share that information with CVS pharmacies for marketing purposes. In its Notice of Privacy Practices, CVS Caremark indeed characterizes itself as an affiliated group of pharmacies that is treated as a single entity for purposes of information sharing.[119] Loopholes such as these, along with the risk of re-identification, necessitate the creation of a comprehensive federal statute designed to protect patient's prescription PHI privacy.[120]

V. PROPOSED FEDERAL PATIENT PRIVACY LEGISLATION

[115] Complaint at 2, Muecke Co. v. CVS Caremark Corp., No. 6:10-cv-78 (S.D. Tex. Sept. 30, 2010).
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] Complaint, Burton's Pharmacy, Inc. v. CVS Caremark Corp., No. 1:11-cv-1 (M.D.N.C. Jan 3, 2011).
[120] Smith, *supra* note 30 at 987.

The *Sorrell* decision implies that the government cannot engage in "content" or viewpoint" discrimination against marketers by prohibiting the commercial use of this data while allowing its non-commercial use.[121] Essentially, the government cannot regulate marketing and other commercial speech differently than other types of speech simply because the speaker is a corporation or the content of the speech is commercial.[122] Under *Sorrell*, legislatures cannot regulate the commercial use of data differently than non-commercial use, which seemingly grants data miners the First Amendment right to use or sell private health information.[123] The New England statutes plainly discriminated against the content and viewpoint of detailer's and were held to violate freedom of speech, and similar statutes will likely be struck down. The current patchwork of laws is inadequate and only protects some consumer data. However, there remains significant government interest in regulating consumer data privacy, as evidenced by California's proposed Do Not Track legislation.[124] This proposed act prohibits the general collection of data that belongs to consumers who have opted out of online tracking, and does not specifically target the commercial use of consumer data, making it acceptable under *Sorrell*.[125] Nevertheless, the act provides broad exceptions for law enforcement, government, and research uses, thus making it possible to discriminate against commercial data use.[126]

The *Sorrell* Court recognized that with the increasing capacity for technology to find and publish personal information, serious and unresolved issues with respect to personal privacy and

---

[121] Katie Booth, *The All-or-Nothing Approach to Data Privacy:* Sorrell v. IMS Health, Citizens United, *and the Future of Online Data Privacy Legislation*, HARV. J.L. & TECH., JOLT Digest, (Aug. 17, 2011), http://jolt.law.harvard.edu/digest/privacy/the-all-or-nothing-approach-to-data-privacy-sorrell-v-ims-health-citizens-united-and-the-future-of-online-data-privacy-legislation.
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] *Id.*

dignity remain. Notably, the court leaves room for new legislation, stating that "[i]f Vermont's statute provided that prescriber-identifying information could not be sold or disclosed except in narrow circumstances then the State might have a stronger position."[127] Thus, it is possible that the court may accept a statute that provides patient privacy through a more narrowly tailored means of restricting data.[128] For instance, legislatures may want to consider universal opt-in or opt-out schemes that allow consumers to choose when and for what purposes their personal data can be used. The Court mentions using HIPAA as such an approach.[129]

Under HIPAA, health care providers and other covered entities are required to "give individuals an understandable notice of the way in which personal health information will be used and disclosed," and to "make a good faith effort to obtain a written acknowledgement of receipt of notice."[130] All healthcare providers must provide patients with notice of privacy practices and obtain written acknowledgement of these practices.[131] Once providers have given notice and received consent, personal health information can be used for treatment, payment, and healthcare operations purposes without further permission.[132] All entities that wish to use patients' data must inform the patient *ex ante* of all the ways their data will be used.[133] This process resembles a universal "opt-in" scheme that applies to both commercial and non-commercial entities that might pass muster under the *Sorrell* Court.[134]

A. The Need for Patient Centered Protection

---

[127] *Sorrell*, 131 S. Ct. at 2659.
[128] *Id.*
[129] *Id.* at 2668.
[130] Booth, *supra* note 121.
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Id.*

Current laws create a system that allows pharmacies and data companies, rather than patients, to own and control personal health data. Patients have a legitimate interest in protecting prescription PHI that may reveal intimate details about their life and health. In particular, patients currently lack protection for the privacy of their de-identified or encrypted prescription PHI. HIPAA only applies to identifiable PHI and is more focused on simply providing notice to patients regarding use of their PHI rather than allowing the patient to consent to such use. Although PHI used by data mining companies is facially de-identified, advances in computer science compromise the power of de-identification processes.[135] A patient-centric approach would empower patients to choose how data miners and pharmaceutical companies use their prescription PHI.

B. Benefit of Federal Level Legislation

Any future statutory attempts to protect patient prescription PHI should be made at a federal level for several reasons. First, a federal statute will create uniformity that will allow courts to apply the same laws across the board as applied to prescription information sharing.[136] This uniformity will be valuable to patients who may be subjected to different PHI privacy laws by simply moving between states.[137] The uniformity will also reflect the nature of the emerging health care system, which rapidly accesses and interprets internet-based health records that may be transmitted from several different locations. [138]

---

[135] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failures in Anonymization*, 57 UCLA L. REV. 1701, 1716 (2010).
[136] Elizabeth Hutton & Devin Barry, *Privacy Year in Review: Developments in HIPAA*, J.L. & POL'Y INFO. SOC'Y 347, 379 (2005) (arguing that additional federal legislation is needed to uniformly protect patient privacy because HIPAA fails to preempt state law).
[137] Mowery, *supra* note 101, at 718-19 (noting that varying state privacy laws create problems for patients who move from one state to another).
[138] Mowery, *supra* note 101, at 739.

In addition to benefitting patients, a federal level statute will streamline processes for covered entities that may otherwise struggle to comply with different levels of protection among different states. In particular, large nationwide corporations will only have to comply with one clear set of regulations, rather than dealing with the burden of meeting different state requirements. [139] A federal standard will also help to create clear compliance standards and enforcement practices. In terms of potential costs savings, efficiency, and simplicity, a federal law that completely preempts state law would provide the most benefits.

C. Opt-in With Consent as a Major Requirement

Current federal and state laws only provide reactive privacy protection, meaning that patients are not able to prevent unauthorized access to their prescription PHI but are only able to file suit after a breach of privacy occurs. Future legislation to protection patient prescription PHI should allow the patients a priori to choose if and how their information is used. A universal opt-in scheme that applies to both commercial and non-commercial entities may protect patient data and offer patients granular control over their information. This type of approach is utilized by Facebook applications, which are programs created by outside companies that run off Facebook user data.[140] Facebook users who wish to use these applications are presented with a dialogue box that lists exactly what types of personal information the applications will use and asked for permission. This approach offers a degree of transparency and differs from practices used by websites like dictionary.com, which installs hundreds of tracking files on users' computers

[139] Jennifer L. Klocke, *Prescription Records for Sale: Privacy and Free Speech Issues Arising from the Sale of De-Identified Medical Data*, 44 IDAHO L. REV. 511, 535 (2008) (state-by-state regulation may slow interstate commerce as large retail chain pharmacies and other covered entities whose business crosses state borders would have to customize [prescription] data to meet the requirements of each individual state before the data are transferred").
[140] Booth, *supra* note 121.

without notice.[141] The proposed federal legislation to track prescription PHI could mirror Facebook privacy settings and allow patients to opt in to use for research, marketing, insurance purposes. Certain exceptions may be made in public health emergencies, law enforcement, payment, and treatment purposes. Patients should be able to change their preferred settings at any time.

An opt-in scheme that provides several options for how patients would like their prescription PHI released would be likely to pass constitutional First Amendment scrutiny. Opt-in provisions that allow patients to exercise meaningful choice over how their health information is shared are necessary for the proliferation of health IT.[142] Explicit consent systems will allow patients to customize the balance between sharing and confidentiality. In the future, there will ideally be a patient consent system that is editable over the internet and accessible by authorized record holders.[143] Future legislation to protection prescription PHI should also include mechanisms that allow patients to track where their data goes and allow them to change their preferences at any time. This may be accomplished by creating software that assigns patients to codes that allow them and authorized users to track their information, whether it is identifiable, de-identified, or encrypted. The tracking system must be secured against hacking and allow patients and government regulators to detect breaches of PHI. Finally, HHS should reinforce the deterrence of improper use by conducting audits of the tracking system. Patient empowerment and government enforcement should deter violations of patient privacy.

---

[141] *Id.*
[142] The MITRE Corporation, *Meaningful choice: Enabling Patients to Selectively Manage Access to their Health Records*, Thought Leadership (July 2011), http://www.mitre.org/work/health/downloads/privacy.pdf.
[143] Arnon Rosenthal, *Digital Policies for Patient Consents: the thorny (and general) Technical Challenges*, the MITRE Corporation (July 2011), http://www.mitre.org/work/tech_papers/2011/11_2001/.

D. Obstacles to Implementation of a New Federal Statute

If the federal government chooses to pass an opt-in data privacy law in the wake of *Sorrell*, it will face the tough challenge of deciding whether data privacy is worth the risk to innovation and research.[144] Opt-in data privacy schemes may negatively impact research, innovation, and even privacy.[145] For instance, one effect of an opt-in scheme for data privacy is that it creates a dual cost structure in which the user must decide first if it is worth the time to make the decision to opt-in; and second, whether the value of the service justifies the decision to opt-in.[146] This decision making process may have the effect of imposing a cost on the initial recognition of a valuable opportunity or service, which may decrease the use of new services and stifle innovation.[147] Further, an opt-in scheme may create a demand for "single identity systems" that allow users to use the same account to log in to multiple website, which would have an excessive scope and would likely result in less consumer privacy.[148] Next, consumers may become desensitized after multiple data requests so that as the scope of data requests become broader without awareness on the part of the user. Another potential negative effect would be "balkanization," which is a scenario where users may become reluctant to leave a service that they have invested in and evaluated, which would result in a decrease in data mobility and a subsequent decrease in consumer value and competition.[149]

---

[144] Booth, *supra* note 121.
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *Id.*
[149] *Id.*

Open-data advocates have argued that patient privacy laws are paternalistic and harmful to business and innovation.[150] Currently, there are many means to obtain personal health information outside of medical records or prescription PHI, such as through credit card purchases or behavioral patterns.[151] These methods are readily available and are not covered by HIPAA, making efforts to truly anonymize data practically futile. Moreover, the de-identification and anonymization of data may prevent it from being useful. Open-data proponents suggest that medical professionals and commercial aggregators of data could continue to use health data effectively by being honest about how consumers' data will be used.[152] This type of system is supported by the proposed opt-in scheme that provides clear consent forms and mechanisms that allow patients to control the dissemination of their own data. Patients who are confident about how their data will be used may be more likely to share it, supporting the reusability, portability, and integration of data.

State legislation and services like Google+ have demonstrated that consumers want to share data categorically for some purposes but not with others.[153] However, *Sorrell* prohibits legislatures from tailoring data privacy laws to protect the use of data from commercial use. *Sorrell's* core rule, that laws must regulate commercial use of data in the same manner as non-commercial use, implies that schemes that apply universally to all data users, such as an opt-in scheme, will be acceptable. However, present legislatures and users may not want to take the step of a universal opt-in scheme. The new statute would present many obstacles to implementation, the primary one being the costs of creating an effective tracking system. Further,

---

[150] Anna Azvolinsky, *Open-Data Advocate Says Health Information Must Be Shared*, NY Genome Center (Dec. 10, 2012), *http://www.nygenome.org/blog/open-data-advocate-says-health-information-must-be-shared*.
[151] Azvolinsky, *supra* note 150.
[152] *Id.*
[153] Booth, *supra* note 121.

a universal opt-in scheme may reduce desirable uses of health data, such as for public health reports. Reducing the free flow of data may also stifle innovation and harm customer value. Ultimately, the federal government may be unable to enact a universal scheme and may leave consumer data privacy to private market or state control. Because legislation may fail to adapt to new technology and may impose heavy financial burdens, many believe that market regulation is preferable to government regulation.[154] Private market data privacy policies, which can make categorical distinctions among different types of data use, may be a sensible option in the wake of *Sorrell*.

CONCLUSION

Current federal and state laws are inadequate for protecting the privacy of patient prescription PHI. The exponential growth of electronic health records and electronically coded data, and the weakness of existing state and federal privacy laws, necessitate the creation of a comprehensive, patient-centered privacy statute that empowers patients to control and protect their patient prescription PHI. This new law should also be designed to give stronger protection to de-identified or encrypted PHI, which has been largely neglected by existing law. The re-identification or unencryption of this data can reveal details about the patients' health and lifestyle and subject them to unfair treatment by insurers and employers, as well as cause embarrassment and stress.

The *Sorrell* Court decision implied that future legislative attempts to protect prescription information privacy may be acceptable if they provided narrow and well-justified privacy exceptions. A comprehensive, patient-centric federal level statute can uniformly protect the privacy of prescription PHI in both identified and unidentified forms. The proposed statute will

---

[154] *Id.*

allow patients to exercise granular control over their own data through an opt-in scheme that is transparent and well enforced. This type of statute is needed to empower patients to confidently share their information and support the legitimate use of data to improve clinical outcomes.