NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 10
Issue 3 *Online Issue*

Article 7

10-1-2008

IMS Health, Inc. v. Ayotte: Small Step for Privacy, Giant Leap Still Needed for Prescription Data Privacy

Kathryn M. Marchesini

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
10 N.C. J.L.& TECH. ON. 96 (2009)

IMS HEALTH, INC. V. AYOTTE: SMALL STEP FOR PRIVACY, GIANT LEAP STILL NEEDED FOR PRESCRIPTION DATA PRIVACY

Kathryn M. Marchesini[1]

Electronic data use in United States industries provides a means by which businesses aggregate, track, and manage consumer information. In the health care industry, data mining companies, pharmacies, and pharmaceutical manufacturers have adopted electronic data use with prescription information. The use of electronic prescription data as a commodity raises privacy concerns which have prompted the formation of state laws restricting its use. Data mining companies recently challenged a New Hampshire law restricting the commercial use of prescription data. In IMS Health, Inc. and Verispan, L.L.C. v. Kelly A. Ayotte *the First Circuit held that a state has the right to prohibit the transfer, sale, and use of patient and prescriber-identifiable drug data for commercial purposes. This Recent Development examines the authority of and need for Congress to enact federal legislation to achieve effective prescription data privacy, augmenting New Hampshire's law and ensuring privacy throughout the country. This analysis considers the effects of the court's narrow statutory interpretation and extent to which states can curtail the commercial use of prescription data. Moreover, existing federal health information privacy protections do not go far enough to protect prescriber-identifiable data, and federal law should address the gap, especially as the health care industry transforms and data management becomes borderless.*

I. INTRODUCTION

Many United States industries, including health care, use electronic personal data to provide business intelligence.[2] Using

[1] J.D. Candidate, University of North Carolina School of Law, 2010.

technology, companies gather, store, and analyze data to assist business operations.[3] For example, regardless of how retail pharmacies[4] obtain information to fill prescriptions,[5] most pharmacies electronically store prescription data in databases.[6] Not only does this stored data contain the type and brand of drug, dosage, and quantity dispensed, it includes the patient's name and the prescriber's identity.[7] Data mining companies[8] purchase electronically stored prescription data from pharmacies and aggregate, manipulate, and sell the modified prescription data to pharmaceutical manufacturers.[9] Through a business practice

---

[2] *See, e.g.,* WEBSTER'S NEW MILLENNIUM DICTIONARY OF ENGLISH, (Preview ed. (v. 0.9.7) 2009), http://dictionary.reference.com/browse/business (defining business intelligence as "the process of gathering information about a business or industry matter; a broad range of applications and technologies for gathering, storing, analyzing, and providing access to data to help make business decisions") (last visited Apr. 1, 2009) (on file with the North Carolina Journal of Law & Technology).

[3] *Id.*

[4] Pharmacies, insurance companies, and electronic transmission intermediaries acquire and store data as part of the business they conduct. *See* IMS Health, Inc. v. Ayotte, 550 F.3d 42, 73–74 (1st Cir. 2008), *petition for cert. filed*, 2009 WL 797587 (U.S. Mar. 27, 2009) (No. 08-1202).

[5] Patients and doctors can submit information by paper, phone calls, or e-prescribing. *See generally* Department of Health and Human Services, Overview E-prescribing, http://www.cms.hhs.gov/eprescribing/ (last visited Apr. 1, 2009) (on file with the North Carolina Journal of Law & Technology) (defining e-prescribing as "a prescriber's ability to electronically send an accurate, error-free, and understandable prescription directly to a pharmacy from the point-of-care").

[6] *See generally* ROBERT P. NAVARRO, ESSENTIALS OF MANAGED HEALTH CARE, 299-303 (Peter R. Kongstvedt ed., Jones and Bartlett Publishers 2003) (discussing pharmacy information systems and health informatics).

[7] *IMS Health*, 550 F.3d at 45.

[8] These companies purchase and compile prescription data in order to sell the data to research and academic institutions, law enforcement agencies, and private organizations. *See* Electronic Privacy Information Center (EPIC) – IMS Health v. Ayotte, http://epic.org/privacy/imshealth/ (last visited Apr. 1, 2009) (on file with the North Carolina Journal of Law & Technology).

[9] *IMS Health*, 550 F.3d at 45 ("[T]hey purchase data . . . aggregate the entries, group them by prescriber, and cross-reference each physician's prescribing history with physician-specific information available through the American

known as "detailing,"[10] pharmaceutical sales representatives use prescription data to conduct target marketing toward specific doctors.[11]

Federal privacy protections provided by the Privacy Rule,[12] promulgated under the Health Insurance Portability and Accountability Act (HIPAA),[13] govern patients' protected health information ("PHI").[14] Pharmacies are not allowed to disclose PHI

Medical Association. The final product enumerates the prescriber's identity and specialty, the drug prescribed, and kindred information.").

[10] Detailing occurs when a pharmaceutical representative communicates with a health care professional to provide pharmaceutical information and promote a pharmaceutical product. Traditionally, pharmaceutical detailing involves face-to-face communication; however, there has been increased use of information technology through e-detailing. *See generally* Press Release, Manhattan Research, L.L.C., Big Changes Ahead for Technology-Based Pharmaceutical Detailing, Nov. 10, 2004, http://www.manhattanresearch.com/newsroom/Press_Release/eDetailing_11102004.aspx (last visited Mar. 9, 2009) (describing technology-supported detailing) (on file with the North Carolina Journal of Law & Technology). *See also IMS Health*, 550 F.3d at 44–45.

[11] *See IMS Health*, 550 F.3d at 45.

[12] *See* 45 C.F.R. §§ 164.514 (2008) (establishing regulations for the use and disclosure of PHI). There is no mention of prescriber-identifiable prescription data. *See id.*

[13] The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–91, §§ 261–64 (1996) [hereinafter HIPAA]. The law's primary purpose is to provide health insurance portability for individuals, with agency rules focusing on the privacy of individuals' health information. *See* U.S. Department of Health and Human Services—Office for Civil Rights (OCR), *Summary of the HIPAA Privacy Rule,* (2003) [hereinafter *Summary of the HIPAA Privacy Rule*], *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf ("The *Standards for Privacy of Individually Identifiable Health Information* ('Privacy Rule') establishes . . . a set of national standards for the protection of certain health information . . . . The Privacy Rule standards address the use and disclosure of individuals' health information—called 'protected health information' by organizations subject to the Privacy Rule—called 'covered entities,' as well as standards for individuals' privacy rights to understand and control how their health information is used.").

[14] PHI includes any information about health status, provision of health care, or payment for health care that can be linked to an individual. Eighteen identifiers constitute PHI, including name, e-mail, and social security number. Data is considered de-identified (and may be used) if all of these identifiers are removed. *See* 45 C.F.R. § 164.514(b)(2) (2007).

to a third party,[15] except as expressly permitted by the Privacy Rule.[16] The HIPAA Privacy Rule, however, does not prevent pharmacies from disclosing prescriber-identifiable prescription data.[17] Therefore, data-miners can purchase and sell prescriber-identifiable prescription data from pharmacies, allowing for detailing to occur.

Although the sale of electronic prescription data is a lucrative business[18] and drug companies consider this data an invaluable resource,[19] the data's transfer and use have implications for a prescriber's privacy. Prescribers have the right to be left alone.[20]

---

[15] Pharmacies that transmit health care information are "covered entities" within the meaning of the HIPAA Privacy Rule because they are "health care providers" that transmit "health information" in electronic form in connections with a "transaction" covered by HIPAA. *See* 45 C.F.R. § 160.103 (2008). They provide a health service by filling prescriptions and then billing a consumer's health insurance company for its portion of the prescription's cost. *See* §§ 45 C.F.R. 160.130, 164.502(c) (2007) (requiring covered entities utilizing PHI to de-identify the information and comply with the disclosure provisions of the Privacy Rule).

[16] *See* 45 C.F.R. §§ 160.102, 164.502(c) (2007) (Pharmacies can disclose PHI to data mining companies if they de-identify it in accordance with the de-identification rules). *See also* American Recovery Reinvestment Act of 2009 (ARRA), Health Information Technology for Economic and Clinical Health Act (HITECH Act), 111 Pub. L. No. 5, § 13405, 123 Stat. 115 (2009) (stating that a covered entity or business associate cannot directly or indirectly receive payment for any PHI unless it first obtains a valid authorization from the individual whose PHI is to be disclosed).

[17] PHI does not include prescriber-identifiable data. *See* HIPAA, *supra* note 13.

[18] Stephanie Saul, *Federal Court Upholds Drug Privacy Law*, N.Y. TIMES, Nov. 19, 2008, at B10, *available at* http://www.nytimes.com/2008/11/19/business/19drug.html.

[19] Associated Press, *NH Prescription Privacy Law Upheld*, BUSINESSWEEK.COM, (Nov. 18, 2008) ("The data compiled by companies like IMS and Verispan is considered invaluable by the tens of thousands of drug company salespeople . . . who use it to identify doctors' drug preferences, whether they favor brand-name medicines over generics, and whether they have been willing to prescribe new drugs to the market.") (on file with the North Carolina Journal of Law & Technology).

[20] *See* Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

Privacy is an individual's ability to decide "when, how, and to what extent information about [him or her] is communicated to others."[21] In essence, once a pharmacy fills a prescription, prescriber privacy rights seem to disappear because pharmacies essentially make this information "public" when they sell prescription data.

Many groups have identified problems associated with health data mining and have taken steps to minimize the commercial use of prescription data.[22] In 2006, New Hampshire enacted a Prescription Information Law, specifically prohibiting certain in-state licenses, sales, uses, or transfers of patient and prescriber-identifiable prescription data for use in detailing.[23] The law was the first of its kind in the nation. The First Circuit's recent

---

[21] DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW, 41 (Erwin Chemerinsky et. al ed., Aspen Publishers 2006) (citing ALAN F. WESTIN, PRIVACY AND FREEDOM (1967)). Many theorists view privacy as the control over personal information. *See, e.g.*, Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change*, 80 CAL. L. REV. 1133, 1810–1990 (1992). *But see* Anita L. Allen, *Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 862 (2000) (viewing the privacy-control paradigm as problematic because of limits on its plausibility).

[22] The Prescription Project, *Prescription Data Mining Fact Sheet*, 2, Nov. 19, 2008, *available at* http://www.prescriptionproject.org/tools/solutions_factsheets/files/0004.pdf ("Physician organizations, patient advocacy groups, and legislators have . . . taken steps . . . in the following states: New Hampshire, . . . Vermont, . . . Maine, . . . Hawaii, Maryland, Massachusetts, Nevada, New York, Washington, and the District of Columbia . . . . All existing or proposed legislation restricts only the sale and use of patient or prescriber data specifically for marketing or commercial purposes. They do not restrict [it] for other purposes, including . . . insurance reimbursement, dispensing prescriptions, utilization review, public health research, law enforcement purposes, controlled substances monitoring, adverse effects reporting, or compliance with Medicaid or private insurance formularies and rules.") (last visited Feb. 13, 2009) (on file with the North Carolina Journal of Law & Technology).

[23] *See* N.H. REV. STAT. ANN. § 318:47-f (2006) [hereinafter *NH Prescription Information Law*]; Rick Valliere, *First Circuit Upholds New Hampshire Law Banning Sale of Doctor Prescription Data*, PRIVACY L. WATCH, Nov. 19, 2008, *available at* http://www.bna.com/products/ip/pwdm.htm (on file with the North Carolina Journal of Law & Technology).

decision in *IMS Health, Inc. v. Ayotte*[24] upheld the controversial Prescription Information Law when challenged by two data mining companies on constitutional grounds. The court held that the law did not violate the First Amendment[25] because the law regulates conduct[26] and did not violate the Commerce Clause[27] because it affects only in-state transactions.[28]

Even though the state law aims to restrict disclosure and use of prescriber-identifiable prescription data, loopholes exist that allow the occurrence of these state-prohibited commercial activities.[29] In turn, Congress should enact a federal law to achieve effective prescription data privacy. Part II of this Recent Development focuses on the New Hampshire Prescription Information Law at issue in the *IMS Health* decision, discussing privacy concerns and the court's overall decision regarding the law's constitutionality. Part III argues that although the *IMS Health* decision constitutes precedent to uphold state laws curbing commercial use of prescriber-identifiable data, even in light of existing federal statutes and regulations protecting health information, threats to privacy remain. Part IV proposes that federal legislation should address this overarching issue, as data mining and pharmaceutical companies are multi-state enterprises by which electronic data exchanges often occur outside the state's borders. Finally, with the increased use of health information technology ("health IT") in the United States, Part V highlights the general need for oversight of and safeguards for prescriber-identifiable data protection.

---

[24] IMS Health, Inc. v. Ayotte, 550 F.3d 42, 46 (1st Cir. 2008), *petition for cert. filed*, 2009 WL 797587 (U.S. Mar. 27, 2009) (No. 08-1202) (upholding the constitutionality of *NH Prescription Information Law*).

[25] U.S. CONST. amend. I. This Recent Development will not explore the First Amendment issues.

[26] *IMS Health*, 550 F.3d at 50–53 (accepting the government's argument that the law regulates conduct rather than commercial speech).

[27] *Id.* at 64.

[28] *See id.* at 62–64.

[29] *See id.* at 103–04 (Lipez, J., dissenting).

II. NEW HAMPSHIRE PRESCRIPTION INFORMATION LAW AND THE IMS HEALTH DECISION

The New Hampshire Prescription Information Law states "[r]ecords relative to prescription information containing patient-identifiable and prescriber-identifiable data shall not be licensed, transferred, used, or sold by any pharmacy benefits manager, insurance company, electronic transmission intermediary, retail, mail order, or Internet pharmacy or other similar entity, for any commercial purpose,"[30] except for certain limited purposes.[31] The state justifies the law by arguing that it has a substantial interest in protecting the privacy interests of its constituents, safeguarding patient health, and promoting containment of prescription drug costs.[32] The foremost concern of this Recent Development is privacy interests.

A. *Privacy Interests, Threats, and Harms*

The aggregation, insecurity, and secondary use of prescription data are forms of information processing that pose a risk to patients and prescribers.[33] While prescription data must be de-identified[34]

---

[30] N.H. REV. STAT. ANN. § 318:47-f (2006) ("Commercial purpose includes, but is not limited to advertising, marketing, promotion, or any activity that could be used to influence sales or market share of a pharmaceutical product, influence or evaluate the prescribing behavior of an individual health care professional, or evaluate the effectiveness of a professional pharmaceutical detailing sales force.").

[31] *Id.* (listing acceptable limited purposes as "pharmacy reimbursement; formulary compliance; care management; utilization review by a health care provider, the patient's insurance provider or the agent of either; health care research; or as otherwise provided by law").

[32] *IMS Health*, 550 F.3d at 47, 75.

[33] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 490 (2006).

[34] *See generally* William Landi & R. Bharat Rao, *Secure De-identification and Re-identification*, American Medical Informatics Association Annual Symposium Proceedings 905 (2003) *available at* http://www.pubmedcentral .nih.gov/articlerender.fcgi?artid=1479909 ("The term *de-identified data* refers to patient data from which all information that could reasonably be used to identify the patient has been removed (e.g., removing name, address, social security

to protect patient privacy,[35] the risk of re-identification remains.[36] For instance, the potential secondary use[37] and sharing of prescription data with a data-miner could cause harm to the dignity of a patient or prescriber.[38] This Recent Development focuses on the privacy interests of prescribers.[39]

In addition to the health care industry's cultural norms and the sensitive nature of health information, prescribers have no desire for data-miners and/or detailers to have access to their prescribing behavior.[40] Government officials, as third parties, do have access

---

number, etc. . .).") (on file with the North Carolina Journal of Law & Technology).

[35] The HIPAA Privacy Rule forbids pharmacies to disclose patient-identifiable information to data mining companies without express patient authorization to do so. *See* 45 C.F.R. § 164.508(a)(3) (2007).

[36] *See generally* Supplemental Brief for the Electronic Privacy Information Center et al. as Amici Curiae Supporting Defendant-Appellant at 6. IMS Health, Inc. v. Ayotte, No. 07-1945 (1st Cir. Aug. 20, 2007) (arguing that de-identified data can be easily re-identified by linking to public records, as one researcher was able to identify eighty-seven percent of the United States population through the use of birth, gender, and zip code information); Christine Porter, *De-Identified Data and Third Party Data Mining: The Risk of Re-Identication of Personal Information*, 5 SHIDLER J.L. COM. & TECH. 3 (2008).

[37] *See* Solove, *supra* note 33, at 521–22 ("'Secondary use' is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent . . . . The harm is a dignitary one, emerging from denying people control over the future use of their data, which can be used in ways that have significant effects on their lives.").

[38] *See* Brandeis & Warren, *supra* note 20, at 197, 214.

[39] To the extent the law prohibits pharmacies from selling or otherwise disclosing patient-identifiable prescription data for commercial purposes, HIPAA provides for the protection of patient health information. *See* HIPAA, *supra* note 13. *See also* U.S. Dept. of Health and Human Services (HHS) Office for Civil Rights (OCR), Health Information Privacy Resolution Agreement, (Jan. 15, 2009) *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresagrcap.pdf. To settle potential violations of the HIPAA Privacy Rule, CVS agreed to pay $2.25 million in a case regarding protected health information. *Id.*

[40] *See generally* Saul, *supra* note 18 ("Such legislation has been urged by doctors who object to the disclosure of their prescribing patterns.").

to prescriber-identifiable data for specific public health reasons.[41] However, disclosing data to third-party data-miners for commercial purposes invades a prescriber's privacy.[42] The data provides details about prescribers' prescription behavior, enabling detailers "to zero in on physicians who regularly prescribe competitors' drugs, . . . large quantities of drugs for particular conditions, . . . and 'early adopters.'"[43] Moreover, under the doctor-patient relationship,[44] patients likely consider prescription data as private.[45] In turn, prescribers could suffer reputational harm because patients may question whether a prescriber's overall basis for prescribing a particular brand-name drug is a medical reason, or a preference resulting from a personal solicitation. New

---

[41] *See, e.g.,* Comprehensive Drug Abuse Prevention and Control Act, 21 U.S.C. § 801 (2006); National All Schedules Prescription Electronic Reporting Act (NASPER), Pub. L. No. 109–60, 119 Stat. 1979 (2005). Thirty-eight states have enacted legislation for prescription drug monitoring programs (PDMPs) to monitor the illegal use of prescriptions for narcotics and other controlled substances. *See generally* U.S. Dept. of Justice, Drug Enforcement Agency, Office of Diversion Control, *State Prescription Drug Monitoring Programs, Questions and Answers,* http://www.deadiversion.usdoj.gov/faq /rx_monitor.htm #1 (last visited Mar. 10, 2008) (on file with the North Carolina Journal of Law & Technology).

[42] *See* Solove, *supra* note 21.

[43] IMS Health, Inc. v. Ayotte, 550 F.3d 42, 47 (1st Cir. 2008), *petition for cert. filed*, 2009 WL 797587 (U.S. Mar. 27, 2009) (No. 08-1202) (defining early adopters as "physicians with a demonstrated openness to prescribing drugs that have just come onto the market").

[44] *See, e.g.,* Vanessa Ho, *Bill Would Make Prescription Data Private,* (Jan. 23, 2009) Seattle Post-Intelligencer Blogs, http://blog.seattlepi.nwsource.com/ healthreport/archives/160219.asp ("The sharing of prescription information for marketing purposes without consent seems to violate the spirit of privacy law, and destroys the confidentiality of the doctor-patient relationship.") (last visited Feb. 15, 2009) (on file with the North Carolina Journal of Law & Technology).

[45] Patients have an expectation of privacy to the extent prescription information is not needed to fill a prescription or process an insurance claim. *See, e.g.*, Donald Nelson, *Why Does Medicine Need Standards?*, (Aug. 1997), Medical Computing Today, http://www.medicalcomputing.org/archives/0astand why.php ("Associating data with the wrong patient is potentially dangerous, and disclosing data to inappropriate recipients violates the patient's expectation of privacy and the professional's commitment to confidentiality.") (last visited May 27, 2009).

Hampshire's concern is the exploitation of the mined data by pharmaceutical detailers that utilize the massive collection of prescription data in marketing brand-name drugs to prescribers.[46]

B. *IMS Health Decision*

IMS Health, Inc. and Verispan, L.L.C., companies in the health data mining business, challenged the Prescription Information Law on First Amendment and Commerce Clause grounds, claiming that the law infringed on commercial free speech[47] and regulated activity wholly outside New Hampshire.[48] As the Commerce Clause prevents state governments from burdening the free flow of goods from one state to another,[49] a law that purports to regulate conduct occurring wholly outside the enacting state "outstrips the limits of the enacting state's constitutional authority and, therefore, is per se invalid."[50] Although the law does not provide explicit geographic limitations, the court narrowly interpreted the law's scope to be the regulation of in-state transactions.[51] Since the Prescription Information Law only regulates in-state commercial

---

[46] *IMS Health*, 550 F.3d at 46.

[47] *Id.* at 48. The First Circuit Court held that the statute provision principally regulated conduct, not speech. *Id.* at 52. Additionally, the law is of no First Amendment significance because the challenged provision only restricts the data-miner's ability "to aggregate, compile, and transfer" information as a commodity. *See id.* at 52–53 (deciding the First Amendment claim on an alternative ground).

[48] *Id.* at 62-63.

[49] *Id.* at 62 (citing Alliance of Auto. Mfrs. v. Gwadosky, 430 F.3d 30, 35 (1st Cir. 2005)).

[50] *Id.* at 62–63 (quoting *Alliance*, 430 F.3d at 35) ("The proper mode of analysis under this so-called 'dormant *Commerce Clause*' depends upon the scope of the challenged statute . . . .").

[51] *See* IMS Health, Inc. v. Ayotte, 550 F.3d 42, 63 (1st Cir. 2008) (1st Cir. 2008), *petition for cert. filed*, 2009 WL 797587 (U.S. Mar. 27, 2009) (No. 08-1202) (citing K-S Pharms., Inc. v. Am. Home Prods. Corp., 962 F.2d 728, 730 (7th Cir. 1992)) ("[S]tate statutes should be presumed to govern only conduct within the borders of the enacting state. . . . [I]t would make no sense to read the statute to regulate out-of-state transactions when the upshot of doing so would be to annul the statute.").

conduct,[52] the majority held that the law did not violate the Commerce Clause.[53]

On the contrary, in *IMS Health*, Judge Kermit Lipez dissented from the majority's Commerce Clause holding, and noted that due to the law's narrow construction, the law's impact in New Hampshire appears "negligible."[54] If the law does not apply outside the state, the law "loses all of its force and effectiveness" because a retail pharmacy in New Hampshire could transfer prescriber-identifiable prescription data to its parent company in another state.[55] The parent company could transfer this data to data-miners outside New Hampshire.[56] No barriers to the use of this data exist for data-miners and detailers.[57] Thus, Judge Lipez would have remanded the issue for further fact-finding regarding the flow of prescriber-identifiable data[58] to determine whether the law violates the dormant Commerce Clause.[59]

---

[52] *Id.* at 63–64 (citing Reply Brief of Appellant at 13, IMS Health, Inc. v. Ayotte, 530 F.3d 42 (1st Cir., 2008)) ("[T]he New Hampshire Attorney General—the state official charged with enforcing its laws—has exhorted us to read the Prescription Information Law to 'relate only to activity that takes place domestically.'").

[53] The Commerce Clause of the U.S. Constitution applies to commerce "among the several States." *See* U.S. CONST. art. I, § 8, cl. 3.

[54] *IMS Health*, 550 F.3d at 104 (Lipez, J., dissenting).

[55] *Id.* at 103.

[56] *Id.*

[57] *Id.*

[58] *See id.* at 106; *see also id.* at 102–03 ("There is a puzzling disconnect between the Attorney General's contention that the Act governs only transactions that take place within New Hampshire and the plaintiffs' contention that all of the conduct that the Act purports to regulate occurs outside the State.").

[59] *IMS Health*, 550 F.3d at 105 (Lipez, J., dissenting) (citing Pharm. Care Mgmt. Ass'n v. Rowe, 429 F.3d 294, 311 (1st Cir. 2005)) ("[T]he dormant *Commerce Clause* . . . is not absolute and in the absence of conflicting legislation by Congress, 'the States retain authority under their general police powers to regulate matters of legitimate local concern, even though interstate commerce may be affected.'"). The dormant Commerce Clause focuses on the extent to which the Commerce Clause constrains a state's interference with interstate commerce, absent federal law. Since there is no federal statute on-point regarding this issue, federal limits apply to state regulation of interstate

III. STATE LAW ADDRESSES ONLY A SUBSET OF A NATIONWIDE DATA PRIVACY ISSUE

A. *Effect and Limited Scope of Prescription Information Law*

As a result of the *IMS Health* decision to uphold the Prescription Information Law, when consumers fill a prescription at a local pharmacy, corresponding prescription data will not be licensed, transferred, sold, or used for commercial purposes within the state of New Hampshire.[60] Nevertheless, the commercial use of prescriber-identifiable prescription data purchased outside the state or transferred for other purposes within the state still threatens the privacy of New Hampshire patients.[61] The *IMS Health* decision undercuts the very privacy concern which the statute was intended to address.[62] The court's narrow interpretation of the law does not fully prevent third parties from accessing prescriber-identifiable data for commercial purposes.[63] An out-of-state commercial data transfer not specifically prohibited[64] would be outside the law's scope.[65] A detailer could buy and use New

---

commerce, prohibiting laws that discriminate against or improperly burden interstate commerce. *See, e.g.*, Gibbons v. Ogden, 22 U.S. 1 (1824).

[60] Sheri Qualters, *1st Circuit Upholds Law Barring Marketers From Using Data on Doctors' Prescriptions*, NAT'L L. J., (Nov. 20, 2008), http://www.law.com/jsp/article.jsp?id=1202426155608 (last visited Feb. 13, 2009) (on file with the North Carolina Journal of Law and Technology).

[61] *See* IMS Health, Inc.. (Lipez, J., dissenting) ("[T]he statute's impact in New Hampshire appears negligible if it truly governs only transactions that occur within the state.").

[62] *See id.* at 47.

[63] *See* Melissa Ngo, *Federal Court Upholds New Hampshire Prescription Privacy Law*, Privacy Lives Blog (Nov. 20, 2008), http://www.privacylives.com/federal-court-upholds-new-hampshire-prescription-privacy-law/2008/11/20/ (last visited Feb. 13, 2009) (on file with the North Carolina Journal of Law & Technology) ("The New Hampshire legislature also noted the privacy interests that patients and physicians have in preventing third parties from receiving in-depth data on every prescription written. . . . [T]here are privacy problems that can arise from 'de-identified data.'"); *id.* at 104 (Lipez, J., dissenting).

[64] *See* § 318:47-f, *supra* note 30.

[65] *See IMS Health*, 550 F.3d at 103–04 (Lipez, J., dissenting) ("It's undisputed that the pharmacy, as a part of its routine practices . . . transfers the information

Hampshire prescriber-identifiable data[66] outside the state for any commercial purpose prohibited within the state,[67] ultimately circumventing the legislature's intent. Hence, a detailer's use of prescriber-identifiable data within the state would not violate the law, as long as the detailer acquires the data outside the state.[68]

The Prescription Information Law seems to be ineffective by design. It restricts the in-state disclosure and use of prescribers' prescribing behavior for target marketing purposes[69] but does not explicitly prohibit detailing.[70] Additionally, the law does not explicitly forbid "the collection, use, transfer, or sale of patient and prescriber de-identified data by zip code, geographic region, or medical specialty for commercial purposes."[71] Consequently, data privacy is still vulnerable to attacks because of sophisticated re-identification programs.[72]

---

in the ordinary course of its business from a data center in the state to data centers outside the state . . . . The explicit language of the Act does not appear to impose such a restriction on the original transfers of data by New Hampshire pharmacies to entities outside the state. Transactions involving those commercial purposes occur farther downstream, and, so far as the record shows, primarily outside the state.").

[66] As an entity covered by the HIPAA regulations, a pharmacy that transmits health care information must de-identify patient health information. *See* 45 C.F.R. § 160.103 (2007).

[67] *See IMS Health*, 550 F.3d at 104 (1st Cir. 2008) (Lipez, J., dissenting), *petition for cert. filed*, 2009 WL 797587 (U.S. Mar. 27, 2009) (No. 08-1202).

[68] *Cf. id.* at 64 (withholding judgment on "whether the purchasers could subsequently make use of the aggregated data in New Hampshire").

[69] Saul, *supra* note 18. *See* N.H. REV. STAT. ANN. § 318:47-f (2006).

[70] *See IMS Health*, 550 F.3d at 103 (Lipez, J., dissenting) ("Because if Rite Aid's pharmacy in New Hampshire can transfer to its parent in Pennsylvania and its parent can transfer to IMS . . . in Pennsylvania, that's not prohibited. And then they can transfer it to Pfizer, wherever Pfizer's headquarters are outside of New Hampshire; and if Pfizer can then use it outside of New Hampshire for all of these various purposes that are prohibited, then there's absolutely no force or effect to this statute.").

[71] *See* N.H. REV. STAT. ANN. § 318:47-f (2006).

[72] Ngo, *supra* note 63 ("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

States regulate the practice of medicine and have jurisdiction over health care licensing requirements.[73] However, a state's ability to regulate the commercial use of prescriber-identifiable data presents a challenge because of the nature of the issue. Due to the free flowing nature of electronic data, prescription data does not adhere to the confines of state borders. In essence, data can be considered borderless. Pharmacies may store prescription data remotely to enable centralized access.[74] The prescription data may not physically reside where it is collected.[75] Thus, an out-of-state transfer of prescription data is often necessary to fill a prescription.[76] Although New Hampshire regulates a physician's ability to write prescriptions, state regulation of unauthorized

---

and death records, incarceration reports, voter registration files, and driver's licensing information.").

[73] State Medical Boards license physicians to practice medicine within the state and provide oversight and disciplinary actions of the overall profession. *See, e.g.*, *New Hampshire Medical Practice Act*, N.H. REV. STAT. ANN. § 329:1, 17 (2008).

[74] Data management practices could be in the form of "Cloud Computing" in which users do not necessarily have control over the technology infrastructure "in the cloud" that support them. *See, e.g., Cloud Computing: The Evolution of Software-as-a-Service*, Knowledge@W.P. Carey, Jun. 4, 2008, http://knowledge.wpcarey.asu.edu/article.cfm?articleid=1614 (on file with the North Carolina Journal of Law & Technology). *See also* Stephanie Condon, *FTC Questions Cloud-Computing Security*, CNET.COM, Mar. 17, 2009, http://news.cnet.com/8301-13578_3-10198577-38.html. The Federal Trade Commission (FTC) is examining the practice of cloud computing and its privacy and security implications. Legislative Hearing on *Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act Before the H. Comm. on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection*, 111th Cong. 16 (2009) (statement of Eileen Harrington, Acting Director of the Bureau of Consumer Protection at the FTC), *available at* http://energycommerce.house.gov/Press_111/20090505/testimony_harrington.pdf (on file with the North Carolina Journal of Law & Technology).

[75] *See id.*

[76] *See* IMS Health, Inc. v. Ayotte, 550 F.3d 42, 102 (1st Cir. 2008), (Lipez, J. dissenting) *petition for cert. filed*, 2009 WL 797587 (U.S. Mar. 27, 2009) (No. 08-1202) ("It is undisputed that none of the *plaintiffs'* transactions take place within New Hampshire . . . . 'IMS and Verispan obtain all of their prescription information, including information on prescriptions filled in New Hampshire, from computers that are located outside of New Hampshire.'").

disclosure and use of prescriber-identifiable data does seem to be effective because the data may not reside within the state's borders. Therefore, federal legislation needs to address this issue.

B. *Existing Information Privacy Case Law, Statutes, & Regulations*

While the Supreme Court has not fully resolved the issue regarding the disclosure of consolidated private data,[77] *Whalen v. Roe*[78] serves as the foundational case for recognizing informational privacy.[79] In *Whalen* the Supreme Court hinted that there may be an individual right to nondisclosure of personal information in certain settings. Although recognized, this informational privacy right is not unlimited.[80] The Supreme Court has yet to define the scope of such privacy protection.[81]

---

[77] Whalen v. Roe, 429 U.S. 589, 605–06 (1977) ("We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions.").

[78] *Id.* at 605 (There is a "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks."); *id.* at 599 (noting that there was an "individual interest in avoiding disclosure of personal matters").

[79] Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records,* 2007 U. ILL. L. REV. 681, 710 (2007).

[80] Several federal courts have held that this constitutionally protected privacy right extends to medical and prescription records. *See, e.g.*, Herring v. Keenan, 218 F.3d 1171, 1175 (10th Cir. 2000); F.E.R. v. Valdez, 58 F.3d 1530, 1535 (10th Cir. 1995) (holding that there was a compelling state interest to prevent Medicaid fraud when psychiatric records were seized pursuant to a state search warrant); Doe v. Southeastern Pennsylvania Transportation Authority, 72 F.3d 1133, 1138 (3rd Cir. 1995) (recognizing a constitutional right to privacy in a patient's prescription records); Lankford v. City of Hobart, 27 F.3d 477, 479–481 (10th Cir. 1994) (noting that police chief's seizure of police dispatcher's medical records from a local hospital without her consent or warrant is an invasion of privacy because it violates the Equal Protection Clause of the Fourteenth Amendment); A.L.A. v. W. Valley City, 26 F.3d 989, 990 (10th Cir. 1994) (noting that an individual's confidential medical information is entitled to constitutional privacy protection when a police officer discloses results of an arrestee's HIV test because an individual has a reasonable expectation of

Technology has played a significant role in the development of information privacy law.[82] To date, Congress has approached the technological assault on privacy in specific industries such as finance, entertainment, and health, by piecemealed consumer privacy protection laws.[83] Although these laws govern the collection, disclosure, and use of certain types of personal data, no federal privacy law[84] comprehensively governs the commercial use and disclosure of prescriber-identifiable prescription data.[85] Even with federal privacy protections provided by the HIPAA Privacy

---

privacy, or he suffered an "injury in fact" as a result of the unlawful disclosures, regardless of the validity of the information). *But see* U.S. v. Sutherland, 143 F. Supp. 2d 609, 613 (W.D. Va. 2001) (holding that individual prescription records from a hospital could be subpoenaed because of the government's interest in obtaining the information was compelling).

[81] *See* Lisa L. Dahm, et al., *Privacy*, *in* E-HEALTH BUSINESS AND TRANSACTIONAL LAW 47, 53 (Barbara Bennett ed., 2002).

[82] *See* Brandeis & Warren, *supra* note 20, at 195 (citing the technology invention of photography as a compelling reason to consider the right to privacy).

[83] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006); Gramm-Leach-Bliley Financial Services Modernization Act, 15 U.S.C. § 6801 (2006); The Video Privacy Protection Act, 18 U.S.C. § 2710 (2006); The Drivers Privacy Protection Act (DPPA), 18 U.S.C. § 2721 (2006); Cable Television Privacy Act, 47 U.S.C. § 551 (2006); Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191, §§ 261-264, 110 Stat. 1936 (1996).

[84] A federal landscape of health-related laws exists that addresses specific issues. However, none of the existing federal laws address the commercial use of prescriber-identifiable prescription data. *See, e.g.*, 45 C.F.R. § 160.103 (2007) (noting that privacy regulations do address and govern the commercial use of prescription data that contains patient-identifiable prescription data); Consolidated Omnibus Budget Reconciliation Act (COBRA), 29 U.S.C. § 1132 (2006); Employee Retirement Income Security Act (ERISA), 29 U.S.C. § 1001 (2006).

[85] *See* Dahm, *supra* note 81, at 54 ("The existing federal laws and regulations that relate to privacy of health information are each limited in some way—either they protect only a specific portion of health information (e.g., substance abuse and treatment records), or they protect the health information of only a portion of the population (e.g., children), or they address only information that is handled electronically (e.g., electronic signatures), or they apply to only particular segment of the health care industry (e.g., 'covered entities').").

Rule,[86] prescriber-identifiable data can be sold to and by data miners.[87] Similarly, no federal regulation de-identification standards exist for prescriber-identifiable prescription data.[88]

Companies' health data mining practices have triggered state legislative action[89] and associated litigation[90] across the United States.[91] The American Medical Association (AMA) has tried to mitigate the threat to privacy through its voluntary, opt-out Physician Data Restriction Program.[92] The program provides physicians with a choice to restrict access to prescription data.[93]

---

[86] *See* Summary of the HIPAA Privacy Rule, *supra* note 13.

[87] *See* 45 C.F.R. § 164.514(b)(2) (2007).

[88] Brief for Defendant-Appellant, *supra* note 36, at 8 ("The closest governing regulation, the Privacy Rule of . . . HIPAA, 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) (2007).

[89] According to the Electronic Privacy Information Center (EPIC), the following states have legislation similar to the New Hampshire law pending (or approved, but not yet effective): Arizona, the District of Columbia, Illinois, Kansas, Maine, Maryland, Massachusetts, New York, North Carolina, Rhode Island, Vermont, Washington, and West Virginia. *See* Electronic Privacy Information Center, IMS Health v. Ayotte, http://epic.org/privacy/imshealth/ (last visited Apr. 2, 2009) (on file with the North Carolina Journal of Law & Technology).

[90] A federal judge in Vermont upheld a state law prohibiting the sale or use of prescriber-identifiable data for the marketing of prescription drugs. IMS Health Inc. v. Sorrell, 2008 U.S. Dist. LEXIS 47454 (D. Vt. Apr. 23, 2009).

[91] Qualters, *supra* note 60.

[92] *See* American Medical Association (AMA), Physician Data Restriction Program, http://www.ama-assn.org/ama/no-index/about-ama/12054.shtml (last visited Apr. 2, 2009) (on file with the North Carolina Journal of Law & Technology).

[93] *Id. Cf.* The Prescription Project, *Prescription Data Mining Fact Sheet*, 3, Nov. 19, 2008, http://www.prescriptionproject.org/tools/solutions_factsheets/files/0004.pdf ("Although the AMA initiated an option in 2006 to allow physicians to 'opt out' of [granting access to their prescribing data], the process is cumbersome and few physicians are aware of the option. Moreover, even when a doctor 'opts out,' the AMA continues to sell that doctor's personally identifiable prescribing information. Pharmaceutical companies may still use the information to target their marketing efforts, as long as they pledge not to provide that individual prescriber's data directly to salespeople. Furthermore,

Furthermore, the pharmaceutical industry recently instituted some restrictions on detailing: pharmaceutical companies must now develop polices regarding the use of prescription data and interactions with health care providers.[94] However, the industry has not gone as far as to ban prescription data use.[95]

IV. FEDERAL PRESCRIPTION INFORMATION PRIVACY REGULATION NEEDED

Similar to the federal statutes and regulations associated with the finance industry—a traditional "paper" industry that has somewhat successfully made the leap into the digital business model—the health care industry could adopt federal laws to handle its intricacies.[96] Particularly, a need exists for a comprehensive, national legal framework regarding the unauthorized commercial use and disclosure of prescriber-identifiable prescription data. To protect against threats to privacy,[97] a federal statute should apply to entities that handle prescriber-identifiable data, regardless of their primary business.[98] Congress could utilize its Commerce Clause

---

the collection of prescribing data and identities through pharmacies is not affected by the AMA policies.") (last visited Apr. 2, 2009) (on file with the North Carolina Journal of Law & Technology).

[94] The Pharmaceutical Research and Manufacturers of America (PhRMA), *PhRMA Code on Interactions with Healthcare Professionals*, http://www.phrma.org/code_on_interactions_with_healthcare_professionals/ (last visited Apr. 2, 2009) (on file with the North Carolina Journal of Law & Technology).

[95] *See id.*

[96] *See, e.g.*, William A. Yasnoff, *Electronic Records Are Key to Health-Care Reform*, BUSINESSWEEK.COM, Dec. 19, 2008, http://www.businessweek.com/print/bwdaily/dnflash/content/dec2008/db20081218_385824.htm (The electronic health record (EHR) is often analogized to a bank account.) (last visited Apr. 2, 2009) (on file with the North Carolina Journal of Law & Technology).

[97] *See, e.g.*, Solove, *supra* note 33. *Cf.* Jennifer Peltz, Associated Press, *Scalia Speaks on Digital Privacy at NYC Conference*, NEWSDAY.COM, Jan. 28, 2009, http://www.newsday.com/news/local/wire/newyork/ny-bc-ny--justicescalia0128jan28,0.4706132.story (U.S. Supreme Court Justice Antonin Scalia notes that "Data such as drug prescriptions probably should be protected . . . suggesting areas off-limits to data gatherers could simply be listed for legal purposes.").

[98] As for potential First Amendment challenges, even if the court considers the transfer or use of prescription data as commercial speech, a federal prescription

power to regulate the use, transfer, license, and sale of prescription data.[99]

Under the Commerce Clause,[100] Congress has complete plenary power when it comes to establishing rules for commercial dealings that concern more than one state.[101] Although Congress' power to regulate interstate commerce is limited,[102] the sale, use, or transfer of prescriber-identifiable data for commercial purposes is an activity that substantially affects interstate commerce.[103] Congress' regulation of prescription data is important to protect the data privacy of prescribers. Even if a state approves prescriber-identifiable data use for commercial purposes, Congress could ban its use as part of comprehensive regulation of pharmaceutical drug selling.[104] Additionally, in a landmark pharmaceutical product liability case,[105] the Supreme Court recently held that the federal drug-approval and warning-label standards[106] do not preempt state

---

information law would likely be constitutional. *See* IMS Health, Inc. v. Ayotte, 550 F.3d 42, 52-53 (1st Cir. 2008), *petition for cert. filed*, 2009 WL 797587 (U.S. Mar. 27, 2009) (No. 08-1202) ("[S]peech-related regulations [exist] that effectively lie beyond the reach of the *First Amendment*.") (emphasis added).

[99] U.S. CONST. art. I, § 8, cl. 3 ("Congress shall have [the] Power . . . [t]o regulate Commerce . . . among the several States.").

[100] *Id.*

[101] *See* Gibbons v. Ogden, 22 U.S. 1 (1824).

[102] *See* United States v. Morrison, 529 U.S. 598 (2000); United States v. Lopez, 514 U.S. 549 (1995) (Congress' power to regulate interstate commerce includes power to regulate: channels of interstate commerce; instrumentalities of interstate commerce; and activities that substantially affect interstate commerce.).

[103] *See* Gonzales v. Raich, 545 U.S. 1 (2005); Wickard v. Filburn, 317 U.S. 111 (1942).

[104] *See generally Gonzales*, 545 U.S. 1.

[105] Wyeth v. Levine, 129 S.Ct. 1187, 1190–92, 1204 (2009). A woman sued a drug manufacturer after the incorrect administration of a drug caused her to develop gangrene in her arm. The Court held that the Food and Drug Administration's (FDA) approval of the pharmaceutical's label does not preempt state law because of Congress's purpose. *Id.*

[106] *See* Federal Food, Drug, and Cosmetic Act (FDCA), 21 U.S.C. §355(a)–(d) (2006). A drug manufacturer may not market a new drug prior to submitting a new drug application to the FDA and receiving its approval. *Id.*

laws.[107] Relying on statutory interpretation,[108] the Court's decision on whether federal laws that regulate certain products "preempt" state tort law tilted toward consumer protection and away from business interest.[109]

While prescription data is within Congress' power to regulate, it may be difficult for Congress to pass a comprehensive law. Due to the internal legislative process, it is often more difficult for Congress to pass a comprehensive legislative scheme than a piecemealed statute. Therefore, in the interim, Congress should expand the scope of the HIPAA Privacy Rule to address the disclosure and use of prescriber-identifiable prescription data. Associated de-identification standards, similar to those protecting PHI,[110] should also be added to protect prescribers.

---

[107] *Wyeth*, 129 S.Ct. at 1204 ("Wyeth has not persuaded us that failure to-warn claims like Levine's obstruct the federal regulation of drug labeling. Congress has repeatedly declined to pre-empt state law, and the FDA's recently adopted position that state tort suits interfere with its statutory mandate is entitled to no weight."); Ashby Jones, *A Big Day for State Tort Laws: A Closer Look at Wyeth v. Levine*, WALL ST. J. L. BLOG, (Mar. 4, 2009), http://blogs.wsj.com/law/2009/03/04/a-big-day-for-state-tort-law-a-closer-look-at-wyeth-v-levine/ (The Court examined the specific statute and determined whether or not it could exist side-by-side with state tort law.) (on file with the North Carolina Journal of Law & Technology).

[108] *Wyeth*, 129 S.Ct. at 1194–95 (citing *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996)) ("[I]n all preemption cases, and particularly in those in which Congress has 'legislated . . . in a field which the States have traditionally occupied,' . . . we 'start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.'").

[109] *See* Ashby Jones, *A Big Day for State Tort Law: A Closer Look at Wyeth v. Levine*, WALL ST. J. L. BLOG, (Mar. 4, 2009), http://blogs.wsj.com/law/2009/03/04/a-big-day-for-state-tort-law-a-closer-look-at-wyeth-v-levine/ ("The Court is going to look at the statutory scheme, make a judgment on whether state action is absolutely incompatible with federal law or not. If there's a tie, the Court, it seems, is going to allow state lawsuits.") (last visited Mar. 10, 2009) (on file with the North Carolina Journal of Law & Technology).

[110] *See* HIPAA, *supra* note 13.

V. CONCLUSION

The New Hampshire Prescription Information Law aims to restrict disclosure and use of prescriber-identifiable data for commercial marketing use.[111] The First Circuit's decision to uphold the state law likely will encourage those states considering similar legislation and create a trend toward increased regulation of prescription data use.[112] If states begin adopting these laws, prescription data mining for commercial purposes would decrease, mitigating threats to data privacy. However, with the court's statutory interpretation in *IMS Health* and the current gap in federal law, every jurisdiction in the United States would need the same prescription information law for another state's law to provide effective comity. Therefore, federal legislation should help address the differences between varying state laws.

While the *IMS Health* decision supports the growing trend to provide prescription information privacy, it seems to "pull the wool over" the ever-increasing issue "of protecting personal information at a time when technology can pull together previously disparate pieces of an individual's history and target advertising by logging a computer user's online travel."[113] Even with the New Hampshire law, the privacy-threatening conduct that the legislature intends to prohibit could still occur. Detailers are still able to use prescribers' histories as targeted-marketing tools to promote the sale of brand-name drugs, as long as detailers obtain prescription data outside state borders.[114] Meanwhile, well-meaning state law may not be effective in protecting prescriber-identifiable prescription data from unauthorized disclosure and use for commercial purposes.[115]

---

[111] *See* N.H. REV. STAT. ANN. § 318:47-f (2006).

[112] *See* EPIC, *supra* note 89.

[113] Peltz, *supra* note 97.

[114] *See* IMS Health, Inc. v. Ayotte, 550 F.3d 42, 55–57 (1st Cir. 2008), *petition for cert. filed*, 2009 WL 797587 (U.S. Mar. 27, 2009) (No. 08-1202) (noting that "pharmaceutical companies use detailing to promote the sale of brand-name drugs, and those drugs cost significantly more than their generic counterparts.").

[115] *See, e.g.*, N.H. REV. STAT. ANN. § 318:47-f (2006).

A national law emulating data protection standards is essential for prescriber-identifiable data, especially as the U.S. health care industry moves toward a Nationwide Health Information Network (NHIN) and increasingly uses electronic health records (EHRs).[116] Similarly, the U.S. Centers for Medicare and Medicaid Services recently promulgated a new electronic prescribing incentive program for physician payment.[117] The program encourages prescribers to trade-in their prescription pads for electronic prescribing when ordering drugs for Medicare patients.[118] Accordingly, in the future, more prescriber-identifiable data will probably be electronically stored and transmitted. As the use of health IT becomes more widespread and systems become interconnected,[119] data management will become increasingly borderless and may exacerbate existing privacy concerns. In the

---

[116] In an overall effort to establish a health information exchange, the U.S. health care industry is developing a Nationwide Health Information Network to make a variety of electronic records interoperable and accessible across the country. *See generally* United States Department of Health and Human Services, Nationwide Health Information Network, http://www.hhs.gov/healthit/healthnetwork/background/ (last visited Apr. 2, 2009) (on file with the North Carolina Journal of Law & Technology). Robert Pear, Privacy Issues Complicates Push to Link Medical Data, N.Y. TIMES, Jan. 18, 2009, at A16, *available at* http://www.nytimes.com/2009/01/18/us/politics/18health.html.

[117] *See* Press Release, Centers for Medicare & Medicaid Services (CMS), *Final 2009 Physician Payment Rule Implements New Electronic Prescribing Incentive Program*, Oct. 30, 2008, http://www.cms.hhs.gov/apps/media/press/release.asp?Counter=3330 ("Approximately 980,000 physicians and non-physicians practitioners (NPPs) bill Medicare under the [Medicare Physician Fee Schedule] (MPFS) for the services they furnish to beneficiaries. Of these, nearly 95 percent accept Medicare's fee schedule rate as payment in full for their services."). *See generally* 73 Fed. Reg. 69847–69852, 2009 Physician Fee Schedule (PFS) Rule (2008). The e-prescribing incentive program is authorized under the Medicare Improvements for Patients and Providers Act of 2008 (MIPPA), § 132 P.L. 110-275 (2008).

[118] *See* CMS, *supra* note 117 ("Physicians . . . [may] earn an incentive payment of 2.0 percent of their total Medicare allowed charges.").

[119] The President recently signed into law statutory provisions that promote health information technology and nationalize adoption of electronic health records. *See* American Recovery Reinvestment Act (ARRA), Health Information Technology for Economic and Clinical Health Act (HITECH Act), 111 Pub. L. No. 5, § 13001, 123 Stat. 115 (2009).

absence of federal regulation of the disclosure and use of prescriber-identifiable prescription data, data mining and detailing business practices will continue threatening prescriber data privacy in order to enable business intelligence.