SOMEBODY'S WATCHING ME: PROTECTING PATIENT PRIVACY IN PRESCRIPTION HEALTH INFORMATION

Christopher R. Smith[*†]

INTRODUCTION

In the 1984 song, "Somebody's Watching Me," Rockwell and Michael Jackson crooned, "I always feel like somebody's watching me/And I have no privacy."[1] Many prescription drug patients would probably be singing the same tune if they knew who was viewing the prescription health information that they provide to their pharmacists and how that information is being used.[2] In today's ever-expanding world of internet technology and electronic data transmission, patient disclosure of prescription health information is being distributed to a widening circle of entities and individuals, raising serious patient privacy concerns, especially when the patient has not given consent to such dissemination.[3]

Recent legislative and judicial attention on the use of prescription data has focused mostly on protecting the privacy of identifiable prescriber information within prescription data and the harm to prescribers resulting from the dissemination and use of such data, not the privacy concerns of patients with regard to the use of such data.[4] By contrast, scholarly analysis

---

* LL.M. 2011, American University Washington College of Law; J.D. 2001, Vanderbilt University Law School; B.A. 1998, University of Richmond. Christopher Smith will be a Visiting Assistant Professor of Law at Widener Law School during the 2012–2013 academic year.

† The author would like to thank John Coster, Ph.D., R.Ph., and Ronna Hauser, Pharm.D., for their support in this effort.

1. ROCKWELL, *Somebody's Watching Me*, *on* SOMEBODY'S WATCHING ME (Motown 1984).

2. Juliana Han, *The Tenth Circuit Finds a Constitutionally Protected Right to Privacy in Prescription Drug Records*, 34 J.L. MED. & ETHICS 134, 135 (2006) (discussing a survey that demonstrated that Americans are concerned about the confidentiality of their PHI); Grace-Marie Mowery, *A Patient's Right of Privacy in Computerized Pharmacy Records*, 66 U. CIN. L. REV. 697, 702 (1998) (noting that most patients are unaware of the third parties who access their prescription information); Arnold J. Rosoff, *The Changing Face of Pharmacy Benefits Management: Information Technology Pursues a Grand Mission*, 42 ST. LOUIS U. L.J. 1, 26 (1998) (noting that most people are uncomfortable with the idea that unknown people may have access to confidential medical records).

3. Harlin G. Adelman & Wendy L. Zahler, *Pharmacist-Patient Privilege and the Disclosure of Prescription Records*, 1 J. PHARM. & L. 127, 128, 130 (1992) (arguing that the expanded use of medical records and computerization of medical data has increased the potential for disclosure of confidential information); Rosoff, *supra* note 2, at 27 (arguing that the use of computers to store medical information has led to greater concern with how easy it is for third parties to access such information, resulting in many patients lacking confidence that their information is well-protected); 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) (arguing that the risk to the privacy of medical records grows with the development of computer technology).

4. IMS Health Inc. v. Sorrell, 630 F.3d 263, 266 (2d Cir. 2010) (demonstrating a focus on a Vermont statute's restriction on the sale, use, or transmission of prescriber-identifiable prescription data in finding the statute unconstitutional); IMS Health Inc. v. Mills, 616 F.3d 7, 12 (1st Cir. 2010)

has focused more on patient privacy within prescription data,[5] but there are few articles examining patient privacy within de-identified patient health data, and most of those do not focus specifically on patient prescription data.[6] Therefore, there is a need for further exploration of the privacy issues surrounding patient prescription personal health information (PHI), especially de-identified patient prescription PHI.

In 2010, Americans filled 3,703,594,389 prescriptions.[7] Each of those prescriptions represents a disclosure of PHI from the patient to others.[8] Every time a patient fills a prescription, the pharmacy collects a host of PHI within its computerized database, including the name of the patient, the patient's address, the date and place the prescription is filled, the patient's

---

(upholding a Maine statute as enacted to protect prescribers' data privacy); IMS Health Inc. v. Ayotte, 550 F.3d 42, 45 (1st Cir. 2008) (upholding a New Hampshire statute that restricts the sale, use, or transmission of prescriber-identifiable prescription data).

5. Han, *supra* note 2, at 134 (analyzing the right to privacy in prescription drug records within the context of the *Douglas v. Dobbs* decision); Michael Heesters, *An Assault on the Business of Pharmaceutical Data Mining*, 11 U. PA. J. BUS. L. 789, 791 (2009) (discussing the potential effects of limiting data mining and potential constitutional solutions to data mining concerns with regard to prescription data); David Orentlicher, *Prescription Data Mining and the Protection of Patients' Interests*, 38 J.L. MED & ETHICS 74 (2010) (addressing the constitutional implications of legislative regulation of data mining); Kathleen A. Ward, *A Dose of Reality: The Prescription for a Limited Constitutional Right to Privacy in Pharmaceutical Records is Examined in* Douglas v. Dobbs, 12 MICH. ST. U. J. MED. & L. 73, 78 (2008) (defending the holding in *Douglas v. Dobbs* as to the scope of patient privacy rights in pharmaceutical data).

6. *Compare* 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 (2008) (discussing the privacy concerns surrounding the use of patient de-identified prescription data), *with* C. Christine Porter, *De-Identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information*, 5 SHIDLER J.L. COM. & TECH. 3, para. 2 (2008), *available at* http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/417/vol5_no1_art3.pdf (discussing re-identification risks of de-identified personal data within a variety of contexts, including the pharmacy context); Nicolas P. Terry, *What's Wrong with Health Privacy*, 5 J. HEALTH & BIOMEDICAL L. 1, 3–4 (2009) (discussing the weakness of the U.S. legal system in addressing de-identification concerns regarding health information); Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers?*, 1 DREXEL L. REV. 216 *passim* (2009) (discussing data de-identification within the context of personal health records).

7. *Total Number of Retail Prescription Drugs Filled at Pharmacies, 2010*, HENRY J. KEISER FAMILY FOUND., http://www.statehealthfacts.org/comparemaptable.jsp?ind=266&cat=5 (last visited Jan. 1, 2012). The United States is the most highly medicated country in the world, and prescription drugs make up 9.4% of all U.S. health spending. Amanda L. Connors, *Big Bad Pharma: An Ethical Analysis of Physician-Directed and Consumer-Directed Marketing Tactics*, 73 ALB. L. REV. 243, 247 (2009) (quoting STEPHEN J. CECCOLI, PILL POLITICS: DRUGS AND THE FDA 165–67 (2004)) (describing the process of developing drugs).

8. Schawbel, *supra* note 3, at 909 (contending that "[e]very day millions of individuals volunteer personal information in order to receive the benefits of health care").

age and gender, the identity of the prescribing physician, the drug prescribed, the drug dosage, and the quantity.[9]

Most patients probably give little thought to disclosing their PHI to pharmacies because they assume that the disclosed information is used by their pharmacist, and perhaps their doctor, for treatment purposes and their insurance companies for purposes of processing the prescription claim and providing coverage.[10] Patients probably think even less about how their prescription PHI is used once it is de-identified.[11] However, patient attitudes might change if patients were more aware of who else sees their prescription PHI or how their PHI is being used.[12]

Regardless of a patient's level of awareness as to how their prescription PHI is being used, serious privacy concerns surround pharmacy transmissions of both identifiable and de-identified PHI to outside entities for purposes other than insurance reimbursement, treatment, public health measures, and law enforcement activity. The list of entities that seek access to patient prescription PHI is quite long, including pharmaceutical manufacturers for marketing purposes, researchers for clinical drug trials, educators, government officials, employers, and lawyers.[13]

This Article lays the groundwork for developing a legal framework to protect the privacy of patient prescription PHI, with a particular focus on de-identified PHI. Part I begins by providing context for why there is need for comprehensive federal legislation to protect patient prescription PHI, including de-identified patient prescription PHI. Part II then outlines the data-mining process for collecting patient prescription PHI and how that data is used. Part III discusses the backdrop of existing federal and state law protecting patient privacy rights, including patient privacy rights in prescription PHI. Part III particularly focuses on three recent state statutory

---

9. *Sorrell*, 630 F.3d at 267 (describing the patient data collected by pharmacies and sold to data miners); *Ayotte*, 550 F.3d at 45 (describing the "potpourri" of patient information stored in pharmacy databases).

10. Mowery, *supra* note 2, at 744 (noting that providers usually "presume that a patient has consented to the disclosure of information if the disclosure is related to providing effective treatment or paying for treatment"); Schawbel, *supra* note 3, at 909 (arguing that individuals who volunteer personal information "rarely question who can access [that] information or for what purpose"); Ward, *supra* note 5, at 75 (arguing that Americans value their privacy in prescription records, particularly when such information is used for purposes other than diagnosis or treatment).

11. *See* Schawbel, *supra* note 3, at 909 ("Many [patients] rarely question who can access [personal health] information or for what purpose it is ultimately used.").

12. *See id.* ("[I]ntensified record keeping has . . . raised questions regarding the access to, and confidentiality of, this stored [personal health] information.").

13. *Sorrell*, 630 F.3d at 268 (describing the purchasers of prescription information data from data miners); IMS Health Inc. v. Mills, 616 F.3d 7, 16 n.4 (1st Cir. 2010) (describing the entities to which data miners sell or license prescription information databases); Schawbel, *supra* note 3, at 918 (describing the variety of entities seeking access to patient prescription drug data).

attempts to directly curb prescription data mining for marketing purposes and the circuit court and Supreme Court responses to those efforts. Part IV evaluates existing state, federal, and related options available for protecting patient prescription PHI against unauthorized disclosure. This Part evaluates the effectiveness of using the state-based data-mining statutes, ethical guidelines, federal constitutional and statutory law, and other state law options for protecting the privacy of patient prescription PHI. Finally, Part V proposes a legislative construct for a federal statute that would allow patients to control the use of and protect their privacy in patient prescription PHI, including de-identified PHI.

I. WHY PROTECTING IDENTIFIABLE AND DE-IDENTIFIED PATIENT PRESCRIPTION PHI IS IMPORTANT

At first glance, the importance of patient privacy in de-identified patient prescription PHI is far from self-evident. After all, de-identified patient prescription PHI is just that, PHI that is de-identified or encrypted prior to being transferred to those not authorized to access the identifiable data.[14] It seems that patients should care less what happens to their data once it is de-identified. This view is overly simplistic.

Complete de-identification of data is becoming an increasingly impossible goal to achieve as all data has a unique signature that *ipso facto* prevents the data from ever becoming truly de-identified.[15] Even data that appears to be completely de-identified can all too easily be re-identified through various processes, such as geo-coding.[16] "Anecdotal evidence suggests [that] algorithms already exist that can re-identify patient information with prescription drug information after third party data mining companies ostensibly de-identify the information."[17]

Compounding the risk of re-identification is the fact that safeguards put into place to protect against attempts at re-identification may not be

---

14. *Mills*, 616 F.3d at 16 (describing how data miners de-identify patient prescription information); *Ayotte*, 550 F.3d at 45 (describing data miners' encryption of patient prescription information to protect patient privacy).

15. Terry, *supra* note 6, at 3 n.8 (citing Gerard Rushton et al., *Geocoding in Cancer Research: A Review*, 30 AM. J. PREVENTIVE MED. S16, S19–20 (2006)) (identifying the growing impossibility of de-identification as the greatest challenge to the de-identification model).

16. *Id.* (discussing the risk of re-identificaiton of de-identified data); Robert Gellman, *The De-identification Dilemma: A Legislative and Contractual Proposal*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 33, 34 (2010) (arguing that "deidentification does not always make reidentification of individuals impossible"); Porter, *supra* note 6, at para. 8 (discussing how publicly available auxiliary information may be used to re-identify anonymized information).

17. Porter, *supra* note 6, at para. 8.

sufficient.[18] For example, the strength of privacy measures is questionable when the entity possessing the de-identified data asserts in its privacy policy that the de-identified data "cannot be linked to personal data by third parties receiving the anonymous information."[19] It is difficult to understand how an entity can confidently make such a bold claim. Even if the company collecting the de-identified data maintains a strong privacy policy, there is no guarantee that a purchaser of such data from that company will maintain a similarly strong privacy policy.[20]

Unfortunately, there exists no national, uniform standard governing the level of identifier-stripping necessary to guarantee that de-identified data cannot be re-identified.[21] In fact, "[n]o matter how many identifiers have been removed or encrypted and no matter how much data has been coded or masked, the remaining data may still be reidentified."[22] The internet makes publicly available an ever-growing amount of personal information, which, in turn, makes it all that much easier to re-identify de-identified personal information.[23] Likewise, once an individual's privacy is breached through re-identification, additional and future re-identification also becomes much easier to accomplish.[24]

Encrypted PHI, as distinguished from de-identified PHI, carries its own set of privacy concerns. First, encryptions are merely codes and almost all codes can be broken.[25] Moreover, encryption requires use of a key or cipher, which is used to lock and unlock the hidden data.[26] Such a key is necessary to allow the hidden data to be viewed in an intelligible manner by those who are authorized to view it.[27] However, there is always a risk that

---

18. *Id.* (discussing how researchers were able to re-identify supposedly anonymous Netflix users who ranked movies on Netflix's website).

19. *Id.* at para. 18.

20. *Id.*

21. Terry, *supra* note 6, at 3 n.9.

22. Gellman, *supra* note 16, at 34–35, 39 (discussing how researchers were able to re-identify supposedly anonymous Netflix users who ranked movies on Netflix's website).

23. *Id.* at 36–37 (noting that an estimated "87% of Americans can be uniquely identified from their date of birth, gender, and five-digit zip code"); Klocke, *supra* note 6, at 520 (stating that remaining information within de-identified data can be matched to other sources of information to re-identify a patient).

24. Porter, *supra* note 6, at para. 12.

25. Todd S. Purdum, *Code Talkers' Story Pops Up Everywhere*, N.Y. TIMES, Oct. 11, 1999, at A14 (explaining that the Navajo code was one of the very few military codes in history to never have been broken).

26. David Colarusso, Note, *Heads in the Cloud, A Coming Storm: The Interplay of Cloud Computing, Encryption and the Fifth Amendment's Protection Against Self-Incrimination*, 17 B.U. J. SCI. & TECH. L. 69, 78–80 (2011) (describing the details of symmetric key encryption and public key encryption).

27. *Id.* at 78 (describing how a cipher or key renders plaintext unreadable gibberish).

the encryption key might fall into the wrong hands, thereby allowing the information to be accessed by unauthorized viewers.[28]

Along with concerns related to security weaknesses, some patients may have subjective privacy concerns regarding encrypted or de-identified patient prescription PHI, even when such information is distributed but remains encrypted or de-identified. For example, even if the individual or entity accessing the prescription PHI of "Patient X" does not know that the information belongs to or is associated with Patient X, Patient X knows that the information belongs to her and knows that someone out there might be viewing that information without her consent. The mere awareness of Patient X that her information is being disseminated without her consent could still cause embarrassment and stress.

By analogy, the scenario is no different than one in which an individual's nude picture is disseminated across the internet without his consent but with the face and other identifying features removed.[29] No one viewing the picture will know the identity of that individual, but that does not mean that the individual does not suffer embarrassment from the knowledge that others are viewing the picture. The issue is one of "'dehumanization' [in] having one's most intimate information circulated by an indifferent and faceless infrastructure without any control over the process or content."[30]

Existing legal protections, such as the Health Insurance Portability and Accountability Act[31] (HIPAA), do not go far enough to protect even identifiable patient prescription PHI, let alone de-identified or encrypted prescription PHI. A couple of recent, pending lawsuits illustrate this concern. These cases arise out of the 2007 merger of the pharmacy chain CVS and the pharmacy benefits manager (PBM) Caremark, which resulted in the merged entity CVS Caremark.[32]

---

28. 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) (outlining the risks of cryptography, including the possibility that encryption keys may not always be kept secret).

29. Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923, 929 (7th Cir. 2004) (opining that a woman whose nude pictures were uploaded to the internet without her consent and without her name would feel that her privacy was invaded if those pictures were viewed by people in a foreign country who did not even know her).

30. Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 298 (2003) (arguing that common law torts provide inadequate protection for informational privacy).

31. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.).

32. Mark Lebovitch & Laura Gundersheim, *"Novel Issues" or a Return to Core Principles? Analyzing the Common Link Between the Delaware Chancery Court's Recent Rulings in Option*

In *Muecke Co. v. CVS Caremark Corp.*, pending in the Southern District of Texas, the plaintiffs allege that Caremark, the PBM side of the CVS Caremark Corporation, while coordinating drug benefits between patients, their insurance companies, and non-CVS pharmacies, collects identifiable prescription health information and transfers that information to CVS pharmacies.[33] According to the complaint, when patients with Caremark as a PBM fill a prescription at a non-CVS pharmacy, the patient's name, address, phone number, social security number, medical diagnosis, prescription history, gender, date of birth, drug dispensed, supply dispensed, and prescriber's name is transmitted to Caremark for purposes of adjudicating the pharmacy claim.[34] Caremark then allegedly shares that information, through an information technology platform, with the CVS or pharmacy side of CVS Caremark.[35]

The plaintiffs allege that once CVS has the patient PHI, it uses the identifiable PHI in ways that would be troubling to many patients. The plaintiffs aver that CVS "accepts payments from drug companies for directly marketing to those patients who are likely candidates for a drug because of their prescription history."[36] The plaintiffs also contend that CVS uses such information to "directly target[] non-CVS patients and solicit[] their business to CVS-owned retail stores and their purchase of CVS-branded over-the-counter products."[37]

A similar scenario is outlined in the North Carolina district court case of *Burton's Pharmacy, Inc. v. CVS Caremark Corp.*[38] In *Burton's Pharmacy*, the plaintiffs allege that CVS uses information from Caremark to contact non-CVS patients by mail, in person, and by phone to market CVS drugs and services directly to those patients.[39] The plaintiffs further claim that CVS "pitches to drug manufacturers its own ability to use this process to market prescription drugs to patients."[40] According to the plaintiffs, some examples of the uses of non-CVS pharmacy patient data include payment by drug manufacturers to CVS to market drugs to the non-CVS pharmacy patients, direct CVS marketing messages to patients that are

---

Backdating and Transactional Cases, 4 N.Y.U. J. L. 505, 532–34 (2008) (providing an overview of the litigation to prevent the CVS Caremark merger).

33. Complaint at 2, Muecke Co. v. CVS Caremark Corp., No. 6:10-cv-78 (S.D. Tex. Sept. 30, 2010).

34. *Id.* at 12–13, 22–24.

35. *Id.* at 14–15, 18.

36. *Id.* at 2; *see also id*. at 16, 20–21, 22, 24.

37. *Id.*; *see also id*. 56, 65–67, 69, 77.

38. Complaint, Burton's Pharmacy, Inc. v. CVS Caremark Corp., No. 1:11-cv-2 (M.D.N.C. Jan. 3, 2011).

39. *Id.* at 10.

40. *Id.*

tailored to specific patient characteristics or demographics, and discount offers to patients for over-the-counter drugs at CVS.[41]

Though HIPAA violations would seem to arise out of the alleged CVS Caremark conduct in these two cases, the plaintiffs in *Burton's Pharmacy* explain how Caremark "claims" to avoid HIPAA violations in sharing the non-CVS pharmacy patient data with CVS pharmacies.[42] The plaintiffs cite CVS Caremark's Notice of Privacy Practices, which states that CVS and Caremark view themselves as part of an affiliated group of pharmacies that is treated as a single entity for purposes of sharing information about patients.[43] In other words, if a patient provides Caremark with authorized access to a patient's prescription PHI, then it can share that information with CVS pharmacies because they are all considered to be a single entity for HIPAA purposes. The plaintiffs allege that CVS Caremark uses the Notice language as a shield against possible privacy concerns raised by CVS's use of non-CVS pharmacy patient data for direct marketing by CVS pharmacies, CVS mail-order pharmacies, and direct marketing by drug manufacturers.[44]

These two cases, along with the privacy policy concerns involving the use of de-identified patient prescription PHI, demonstrate from a policy and practical perspective that existing law fails to adequately protect the privacy of patient prescription PHI, including de-identified patient prescription PHI. The risk of re-identification and decryption, along with loopholes in existing privacy law, justify the need for comprehensive federal legislation to protect patient prescription PHI.

II. THE DATA-MINING AND DETAILING PROCESS

Data mining is a major way in which patient prescription PHI, particularly de-identified PHI, is disclosed, used, and disseminated outside of the pharmacy setting. Data miners are companies that contract with pharmacies, hospitals, and insurance companies to buy their raw data, including patient demographic information and patient drug information, which the pharmacies, hospitals, and insurance companies collect on patients and prescribers.[45] Before the data miners receive this raw data, they

41. *Id.* at 12–13.

42. *Id.* at 11.

43. *Id.*

44. *Id.* at 12.

45. IMS Health Inc. v. Mills, 616 F.3d 7, 16 (1st Cir. 2010) (describing the transfer of prescription data from pharmacies to data miners); Klocke, *supra* note 6, at 512 (describing the data-mining process as increasingly involving the purchase of patient prescription data from hospitals and insurance companies).

install software on pharmacies' computers to encrypt and render anonymous the patient prescription data.[46] Accordingly, the data miners are unable to identify individual patients by name. Nonetheless, data miners can still track patients because they replace the patient's identifying information with a number, which allows them to track the "de-identified" patient over time and correlate that particular patient with the various prescriptions filled by that patient.[47]

Once the data miners receive the raw encrypted data from the pharmacies, they aggregate the available information, categorized by prescriber, and compile reports and databases.[48] These reports and databases allow for the examination of multiple transactions involving the same prescriber to identify that prescriber's "prescribing history, her choice of particular brand-name drugs versus their generic equivalents, and the likelihood she will adopt new brand-name drugs."[49] These databases and reports are very important to brand-name pharmaceutical companies who purchase them from the data miners.[50] The brand-name pharmaceutical companies use the databases and reports to determine their sales representatives' marketing strategies, which are directed at the very same prescribers whose information forms the foundation of the databases and reports.[51] These sales representatives, also known as detailers, use this data to enhance their detailing or sales visits to those prescribers.[52]

There are two primary ways in which data mining specifically enhances detailing. First, the detailers use the aggregate prescriber-specific information "to zero in on physicians who regularly prescribe competitors' drugs, physicians who are prescribing large quantities of drugs for particular conditions, and 'early adopters' (physicians with a demonstrated openness to prescribing drugs that have just come onto the market)."[53] Drug

---

46. IMS Health Inc. v. Sorrell, 630 F.3d 263, 267 (2d Cir. 2010); *Mills*, 616 F.3d at 16; IMS Health Inc. v. Ayotte, 550 F.3d 42, 45 (1st Cir. 2008).

47. Alexander D. Baxter, IMS Health v. Ayotte: *A New Direction on Commercial Speech Cases*, 25 BERKELEY TECH. L.J. 649, 650 (2010) (describing data miners' encryption process); Klocke, *supra* note 6, at 512 (explaining that data miners track patient socioeconomic data).

48. *Mills*, 616 F.3d at 16 (describing how data miners develop a complete picture of prescribers' prescribing history); IMS Health, Inc. v. Ayotte, 550 F.3d 42, 45 (1st Cir. 2008) (describing the scope of the industry in aggregating prescriber data as "mind-boggling").

49. *Mills*, 616 F.3d at 12.

50. *Ayotte*, 550 F.3d at 46–47 (describing the transfer of prescriber prescription data from data miners to brand-name pharmaceutical manufacturers).

51. *Id.* at 47 (describing how prescriber prescription data allows detailers to target prescribers who are prescribing competitor drugs, who are prescribing large quantities of drugs, and who are early prescribers of new drugs on the market).

52. IMS Health Inc. v. Sorrell, 630 F.3d 263, 267 (2d Cir. 2010) (defining the practice of detailing).

53. *Ayotte*, 550 F.3d at 47.

manufacturers and detailers use the databases and reports to focus their marketing efforts on the prescribers who are most likely to maintain brand loyalty to that manufacturer's brand after a patent expires, or who are most likely to prescribe their manufacturer's "patented brand-name drug as against generic drugs, or as against a competitor's patented brand-name drug."[54]

Second, the databases and reports help detailers to more effectively make their sales pitches to prescribers. Knowing a prescriber's prescribing history allows the detailer to hone in on the unique prescribing behaviors of each individual prescriber.[55] For example, the detailer who knows that a prescriber is using a competitor's drug can more effectively craft his or her presentation to highlight the weaknesses of the competitor drug.[56]

Detailers obtain in-person access to prescribers by portraying themselves as educators who can provide prescribers with important new information on research and pharmacological developments.[57] However, some argue that pharmaceutical manufacturers' detailing educational material is very biased with a sole focus on maximizing manufacturer profit and not safely treating the patient.[58] Critics contend that the prescribing of prescription drugs "should be dominated by scientific evidence, not secretive marketing techniques."[59]

Detailers also provide prescribers with about $1 million worth of free drug samples per year, which are highly valued by providers for passing along to patients.[60] Once a detailer obtains access to a provider, the detailer tries to develop an ongoing relationship so that the provider will maintain

---

54. *Id.* at 46; Baxter, *supra* note 47, at 650 (describing pharmaceutical marketers' direct-to-physician approach); Heesters, *supra* note 5, at 795 (describing how Eli Lilly uses data mining to focus on big prescription writers who are most likely to give Eli Lilly the biggest dividend for its investment in detailing).

55. IMS Health Inc. v. Mills, 616 F.3d 7, 14 (1st Cir. 2010) (describing how data miners use prescriber prescription data information to more effectively do their jobs); Joshua Weiss, *Medical Marketing in the United States: A Prescription for Reform*, 79 GEO. WASH. L. REV. 260, 264 (2010) (describing how detailers hone their detailing approaches to prescribers).

56. Orentlicher, *supra* note 5, at 74 (describing how detailers use data-mining prescription data in their presentations to prescribers).

57. *Ayotte*, 550 F.3d at 46 (describing how detailers push past prescriber reluctance to meet with sales representatives).

58. Connors, *supra* note 7, at 262 (describing how Merck's Vioxx detailing materials played down the heart-attack risks of the drug).

59. *Id.* at 277 (arguing that physicians no longer bear the burden to competently and independently research drug safety issues but instead can rely on biased and skewed detailer educational materials).

60. *Ayotte*, 550 F.3d at 46 (describing the value and importance of the free drug samples provided to prescribers by detailers).

brand loyalty to the detailer's manufacturer and continue to prescribe that manufacturer's brand-name drug.[61]

Notably, brand-name drug companies are the sole focus of data mining and the sole source of detailing because detailing is expensive and brand-name drugs, unlike generic drugs, have a high profit margin for the drug manufacturers.[62] Brand-name pharmaceutical companies make annual profits between 15% and 20%, which is far above other industries' profit margins.[63] In 2005, one data-mining company brought in revenues of $1.75 billion through selling prescriber information databases and reports to brand-name drug companies.[64]

Drug manufacturers believe that their detailing efforts are highly effective and that prescribers subject to detailing prescribe the detailed drugs more frequently than alternative generic drugs.[65] Accordingly, it is no surprise that detailing represents a massive marketing campaign.[66] Statistics demonstrate that "the average primary care physician interacts with no fewer than twenty-eight detailers each week and the average specialist interacts with fourteen."[67] Moreover, the Congressional Budget Office has determined that the amount of money spent by drug companies on detailing has more than doubled between 1998 and 2008, with drug companies having spent $12 billion in 2008 on detailing.[68] Shockingly, pharmaceutical

---

61. *Id.* at 46–47 (describing how detailers hook prescribers to develop an ongoing sales relationship with them).

62. IMS Health Inc. v. Sorrell, 630 F.3d 263, 267–68 (2d Cir. 2010) (explaining why detailing is cost-effective for brand-name drug manufacturers only); *Ayotte*, 550 F.3d at 46 (explaining why brand-name drug manufacturers are most active in detailing); Connors, *supra* note 7, at 246 (arguing that the most aggressive marketing is reserved for blockbuster brand-name drugs under patent whose profits exceed all other drugs).

63. Connors, *supra* note 7, at 247 (citing DANIEL CALLAHAN & ANGELA A. WASSUNA, MEDICINE AND THE MARKET: EQUITY V. CHOICE 165 (2006)).

64. IMS Health Inc. v. Mills, 616 F.3d 7, 16 (1st Cir. 2010) (describing IMS Health's data-mining revenues for 2005); Heesters, *supra* note 5, at 793 (noting that data miner ChoicePoint had revenue of $1.1 billion in 2006 and data miner QForma Inc.'s revenue went from $40,000 in 2000 to $2.1 million in 2004).

65. Orentlicher, *supra* note 5, at 76 (highlighting evidence demonstrating that detailing influences prescribing decisions and increases drug sales); Weiss, *supra* note 55, at 262 (arguing that doctors prescribe an advertised drug more frequently once they are subject to detailing).

66. Orentlicher, *supra* note 5, at 74 (characterizing the scope of detailing in terms of participant size and costs).

67. *Ayotte*, 550 F.3d at 47. There is approximately one detailer for every five physicians and $25,000 is spent annually on detailing per physician. Connors, *supra* note 7, at 255.

68. Sheila Campbell, *Promotional Spending for Prescription Drugs*, CONGRESSIONAL BUDGET OFFICE (Dec. 2, 2009), http://cbo.gov/ftpdocs/105xx/doc10522/12-02-DrugPromo_Brief.pdf; *see also* Klocke, *supra* note 6, at 517 (noting that IMS Health has claimed "that winning just one more prescription per week from each prescriber will yield an annual gain of $52 million in sales").

companies spend more on marketing to prescribers than they spend on research or direct-to-consumer advertising.[69]

From the patient's perspective, there are a number of negative implications related to the use and disclosure of de-identified patient prescription PHI through data mining and detailing. First, detailing leads to prescribers overprescribing expensive brand-name drugs when equally effective generic drugs are available, resulting in greater costs to individual patients, insurers, Medicare Part D plans, and Medicaid.[70] This is significant given that total retail drug spending was over $220 billion for 2010[71] and given that the growth rate of brand-name drug costs has been two-to-three times the rate of inflation.[72]

Second, the detailing and resulting overprescribing of brand-name drugs threatens patient health in cases where the effects and potential health risks of generic equivalents are better known than those of newer brand-name drugs.[73] Essentially, detailing causes prescribers to overprescribe unnecessarily risky brand-name drugs to their patients.[74]

Further exacerbating the threat to patient health is the fact that detailing and the free drug samples given to physicians by detailers create a conflict of interest for doctors with regard to their patients.[75] In other words, detailing and the free drug samples can cause doctors to feel more beholden to the drug manufacturer than to their patients. Moreover, if patient health outcomes suffer as a result of detailing-induced prescription decisions, then

---

69. Connors, *supra* note 7, at 246–47 (arguing that putting more funds into marketing than research and development undermines pharmaceutical companies' obligation to find cures for deadly diseases); Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers?*, 1 DREXEL L. REV. 216, 237 (2009) (noting that the pharmaceutical industry spends on marketing twice what it spends on research and development); Weiss, *supra* note 55, at 265.

70. IMS Health Inc. v. Mills, 616 F.3d 7, 17 (1st Cir. 2010) (describing state legislative findings that data mining results in higher health care costs); Orentlicher, *supra* note 5, at 76 (citing studies that demonstrate that, after being subject to detailing, prescribers are more likely to prescribe expensive new drugs over low cost generic drugs, even where there is no medical advantage to the new drug); Weiss, *supra* note 55, at 268–69 (discussing how detailing results in significant overspending by taxpayers and those with insurance).

71. *Total Number of Retail Prescription Drugs Filled at Pharmacies, 2010*, HENRY J. KEISER FAMILY FOUND., http://www.statehealthfacts.org/comparemaptable.jsp?ind=266&cat=5 (last visited Jan. 1, 2012).

72. Baxter, *supra* note 47, at 652 (describing recent prescription drug cost trends).

73. IMS Health Inc. v. Sorrell, 630 F.3d 263, 293 (2d Cir. 2010) (Livingston, J., dissenting) (finding that the risks associated with generic drugs are more well-known than those associated with brand-name drugs).

74. Orentlicher, *supra* note 5, at 75–76 (arguing that patient health may suffer if prescribers become overly enthusiastic about a risky detailed drug and underestimate the side effects of that drug).

75. Connors, *supra* note 7, at 277.

long-term health care costs also rise, including the patient's own costs.[76] Arguably, manufacturer marketing tactics and detailing "has led to an overmedicated society that pays too much money and too little attention [to the benefits and risks of prescription medication]."[77]

For purposes of this Article, the most troubling impact of data mining and detailing is the invasion of patient privacy resulting from the disclosure of both identifiable and de-identified patient prescription PHI. "Americans do not feel that their privacy rights in health care information are adequately protected."[78] Assuming these beliefs are correct, then resulting patient prescription PHI privacy breaches will lead to various negative outcomes for patients, including social and psychological harm through embarrassment, economic harm through job discrimination and job loss, patient difficulty in obtaining health insurance, health care fraud, and patient reluctance to share sensitive information with their doctors or pharmacists.[79] As to the last, inadequate protection of identifiable and de-identified patient prescription PHI chills patient communication with their doctors and pharmacists, hindering the ability of doctors and pharmacists to provide proper counseling to their patients.[80] With these concerns in mind, the next Part of this Article outlines the existing state and federal privacy law framework that applies to the disclosure, dissemination, and use of patient prescription PHI.

---

76. Orentlicher, *supra* note 5, at 75 (arguing that poor prescribing choices may lead to costly hospitalizations).

77. Connors, *supra* note 7, at 277.

78. Schawbel, *supra* note 3, at 911 (quoting Grace-Marie Mowery, Comment, *A Patient's Right of Privacy in Computerized Pharmacy Records*, 66 U. CIN. L. REV. 697, 727 (1998)); *see also* Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 696–97 (2007).

79. Juliana Bell, *Privacy at Risk: Patients Use New Web Products to Store and Share Personal Health Records*, 38 U. BALT. L. REV. 485, 489 (2009) (discussing the negative implications to patients of disclosure of health information); Orentlicher, *supra* note 5, at 76 (addressing the negative impacts when a patient's drug abuse, STD, mental illness, or cancer is disclosed); Schawbel, *supra* note 3, at 911–12 (describing the negative consequences of inadequately protected individual health information); Terry & Francis, *supra* note 78, 696–97 (citing studies of patient behavior to protect their privacy but which can have negative impacts on patient health outcomes).

80. Adelman & Zahler, *supra* note 3, at 152 (arguing that the lack of a pharmacy–patient privilege results in patients being less willing to disclose important medical information to their pharmacists); Schawbel, *supra* note 3, at 947 (discussing how inadequate privacy protections for prescription PHI will interfere with pharmacists' ability to perform their patient counseling obligations under OBRA 1990).

III. FEDERAL AND STATE PRIVACY RIGHTS AND PATIENT PRESCRIPTION PHI

A. State-Based Privacy Rights

The genesis for the state common law right to privacy was the 1890 article, *The Right to Privacy*, by Justice Brandeis and Samuel Warren.[81] Within that article, Brandeis and Warren outlined a common law individual right to privacy, which they characterized as a right "to be let alone."[82] According to Brandeis and Warren, this right to privacy is not founded in contract, property, or trust, but in "inviolate personality," and they argued that such a right to privacy is a right to protect that which is private "as against the world."[83]

While Brandeis and Warren provided a general overview of the common law right to privacy and its corresponding remedies,[84] the more concrete framework was developed in 1960 when Dean William Prosser formally classified the four torts that cumulatively protect the common law right to privacy: intrusion upon seclusion; public disclosure of embarrassing private facts; false light; and appropriation of a plaintiff's name or likeness.[85] Dean Prosser's classification was subsequently adopted in the 1977 *Restatement (Second) of Torts*, which many states have adopted as well.[86] In the context of protecting privacy rights in de-identified prescription PHI, the most likely candidates for a tort suit would be Dean Prosser's intrusion upon seclusion tort[87] and the breach of confidence tort, which is separate and independent from the privacy torts.[88]

---

81. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (providing the doctrinal outline for a legal right to privacy to protect individuals from dangers posed by new technology).

82. *Id.* at 195 (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS: OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACTS 29 (2d ed. 1888)).

83. *Id.* at 205, 213.

84. *Id.* at 214–20.

85. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960) (defining the four tort claims for violation of the common law right to privacy).

86. Trevor Woodage, Note, *Relative Futility: Limits to Genetic Privacy Protection because of the Inability to Prevent Disclosure of Genetic Information by Relatives*, 95 MINN. L. REV. 682, 687 (2010); *see* RESTATEMENT (SECOND) OF TORTS §§ 652B–E (1977).

87. RESTATEMENT (SECOND) OF TORTS § 652B (intrusion upon seclusion requires demonstrating intentional intrusion upon private affairs that would be highly offensive to a reasonable person).

88. Adelman & Zahler, *supra* note 3, at 134 (listing the likely common law torts for protecting against improper disclosure of medical information); Terry, *supra* note 6, at 5–6 (distinguishing between tortious invasion of privacy and breach of confidence, with the former able to be committed by anyone and the latter only able to be committed by one who holds information in confidence); Terry & Francis,

Along with tort actions for invasion of privacy or breach of confidentiality,[89] the state-based right to privacy in PHI is also found within state constitutions[90] and state privacy statutes.[91] With regard to both sources, the case law interpreting the level and type of privacy protection to which prescription PHI is entitled varies, as may be expected, from state to state.

Some states recognize a strong privacy interest in prescription information. For example, a New York appellate court held that pharmacy customers have a reasonable expectation of confidentiality in the health

---

supra note 78, at 712–13 (discussing the application of the breach of confidence tort within the context of health information).

89. Poli v. Mountain Valleys Health Ctrs., Inc., No. 2:05-2015-GEB-KJM, 2006 WL 83378, at *4 (E.D. Cal. Jan. 11, 2006) (denying the pharmacy's motion to dismiss plaintiff's California invasion-of-privacy common law claim against the pharmacy for releasing his prescription records to his employer without his consent); Fanean v. Rite Aid Corp., 984 A.2d 812, 824–25 (Del. Super. Ct. 2009) (recognizing a breach of confidentiality claim when a pharmacy employee disclosed plaintiff's medical information to third parties without justification); Weld v. CVS Pharmacy, Inc., No. CIV. A. 98-0897F, 1999 WL 494114, at *1 (Mass. Super. Ct. June 29, 1999) (denying summary judgment on a pharmacy patient's privacy and confidentiality claims against a pharmacy, mailing service, and drug manufacturers related to a marketing scheme in which the pharmacy disclosed patients' information to a mailing service that sent out drug-manufacturer-funded marketing materials to patients); Anonymous v. CVS Corp., 728 N.Y.S.2d 333, 337 (N.Y. Sup. Ct. 2001) (denying a motion to dismiss a breach-of-confidentiality claim against a pharmacy that sold a HIV patient's prescription information to a chain drug store without the patient's knowledge or consent), *aff'd* 739 N.Y.S.2d 565, 565 (N.Y. App. Div. 2002); *see also* Terry, *supra* note 6, at 5 n.18 (listing state court cases recognizing common law protections for health information).

90. Manela v. Superior Court, 99 Cal. Rptr. 3d 736, 744 (Cal. Ct. App. 2009) (recognizing California constitutional right to privacy in medical records); McEnany v. Ryan, 44 So. 3d 245, 247 (Fla. Dist. Ct. App. 2010) (citing State v. Johnson, 814 So. 2d 390, 393 (Fla. 2002)); Ussery v. Children's Healthcare of Atlanta, Inc., 656 S.E.2d 882, 894–95 (Ga. Ct. App. 2008) (recognizing that personal medical records are protected by a Georgia constitutional right to privacy); Brende v. Hara, 153 P.3d 1109, 1115 (Haw. 2007) (recognizing a privacy right within the Hawaiian state constitution protecting the privacy of highly personal and intimate information contained within medical records); T.L.S. v. Mont. Advocacy Program, 144 P.3d 818, 824 (Mont. 2006) (recognizing Montana's constitutional right to privacy in a patient's medical history); Catherine Louisa Glenn, Note, *Protecting Health Information Privacy: The Case for Self-Regulation of Electronically Held Medical Records*, 53 VAND. L. REV. 1605, 1609, n.25 (2000) (identifying the constitutions of Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington as protecting health information privacy).

91. Lawson v. Meconi, 897 A.2d 740, 745 (Del. 2006) (holding that Delaware's Health Record Privacy Statute protects information contained within an autopsy report from public disclosure); Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 49–50 (Minn. Ct. App. 2009) (holding that Minnesota's statute regarding improper disclosure of patient medical records was not preempted by HIPAA where patient sued provider and provider's employees for posting information on the internet stemming from patient's medical file); Washburn v. Rite Aid Corp., 695 A.2d 495, 498 (R.I. 1997) (holding that a pharmacy's disclosure of a wife's prescription records to her husband's attorney without her knowledge or consent or a court order violated Rhode Island's Confidentiality of Health Care Information Act); *see also* Terry, *supra* note 6, at 6 n.19 (listing state statutes providing for the protection of health information).

information that they provide to their pharmacists.[92] Similarly, in the context of unauthorized use of patient prescription PHI, a Massachusetts trial court recognized causes of action on behalf of pharmacy patients for violations of a state privacy statute, breach of fiduciary duty, breach of confidentiality, and tortious misappropriation of private and personal information.[93] Likewise, the Rhode Island Supreme Court has held that a pharmacy's unauthorized disclosure of a patient's pharmacy records to his wife's attorney, within the context of a divorce proceeding and pursuant to a subpoena, violated the state's Confidentiality of Health Care Information Act and Privacy Act.[94]

On the other hand, the Supreme Court of South Carolina has held that a pharmacist does not owe a pharmacy customer a duty of confidentiality.[95] Likewise, a Louisiana appellate court held that a wife's acquisition of her husband's prescription records from his pharmacy without his consent did not amount to an invasion of privacy because her interest in obtaining the records, in the context of a custody proceeding, outweighed the husband's privacy interest in the records.[96] A Connecticut trial court was even more absolute when it dismissed a patient's invasion of privacy claim against a pharmacy for disclosing his prescription information to law enforcement without a warrant or subpoena.[97] The court based its decision on a Connecticut statute authorizing law enforcement personnel to review patient prescription records, holding that a person does not have any reasonable expectation of privacy in his or her prescription records as to law enforcement, even without probable cause, a subpoena, or a search warrant.[98]

Other courts fall somewhere in the middle of these two extremes. The Supreme Court of Vermont has held that individuals have an expectation of privacy in their pharmacy records, but that a warrantless inspection of the defendant's pharmacy records was sufficiently limited by state law to

---

92. *Anonymous*, 728 N.Y.S.2d at 337 (denying a motion to dismiss filed by a pharmacy that sold an HIV patient's prescription information to a chain drug store without the patient's knowledge or consent).

93. *Weld*, 1999 WL 494114, at *1 (denying summary judgment on a pharmacy patient's privacy and confidentiality claims related to a marketing scheme in which a pharmacy disclosed patients' information to a mailing service that sent out drug-manufacturer-funded marketing materials to patients).

94. *Washburn*, 695 A.2d at 498–500.

95. Evans v. Rite Aid Corp., 478 S.E.2d 846, 847 (S.C. 1996) (holding that a pharmacy did not owe a customer a duty of confidentiality where a pharmacy employee falsely disclosed to others that the customer's prescription was for a venereal disease).

96. Sparks v. Donovan, 884 So. 2d 1276, 1282 (La. Ct. App. 2004).

97. Russo v. CVS Pharmacy, Inc., No. CV020815169S, 2005 WL1097089, at *1 (Conn. Super. Ct. Apr. 5, 2005).

98. *Id.* at *4.

render the inspection reasonable.[99] The Delaware Superior Court held that a pharmacy employee's disclosure of a patient's prescription information may be correctly characterized as a breach of confidentiality claim, but that the same activity would not give rise to an invasion of privacy claim.[100] The court ruled that the former tort is focused on wrongful dissemination of private information, whereas the latter tort is focused on wrongful access to such information, and the pharmacy employee's access to the plaintiff's prescription information was held to be reasonable.[101]

These state cases demonstrate a few important points. First, state courts vary widely in terms of how much protection they afford with regard to a patient's right to privacy within patient prescription PHI.[102] Second, even when state courts recognize a strong privacy interest in patient prescription PHI, common law, statutory law, and state constitutional law differ from state to state, and the courts differ in how they apply that law to protect privacy within patient prescription PHI.[103] Third, there do not appear to be any state court cases that directly address a patient's right to privacy in de-identified patient prescription PHI. All of the above cases seem to focus on privacy rights solely within identifiable patient prescription PHI.

B. The Federal Right to Privacy

1. Federal Statutory and Regulatory Privacy Protection

The federal right to privacy in patient prescription PHI arises out of two sources: (1) the federal statutes and regulations related to health information privacy; and (2) the constitutional right to privacy. The two major[104] federal statutes regarding health information privacy are the Health

---

99. Vermont v. Welch, 160 Vt. 70, 78, 83–84, 624 A.2d 1105, 1109, 1112 (1992).

100. Fanean v. Rite Aid Corp., 984 A.2d 812, 821, 824–25 (Del. Super. Ct. 2009).

101. *Id.* at 821 (holding that the tort of intrusion upon seclusion is focused on the wrongful procurement of private information, not the wrongful dissemination of such information, and that the pharmacy employee's access to the patient's prescription records was reasonable).

102. Mowery, *supra* note 2, at 712 (arguing that a patient's right to privacy is protected on a state level, but the protections vary from state to state).

103. *Id.* (arguing that state "confidentiality requirements vary according to the type of information being held, who is holding the information, and what type of information transaction is involved").

104. The Privacy Act also provides some privacy protection by requiring notification to patients that the government is collecting their health information data and whether or not the disclosure of the data to the government is voluntary or mandatory. However, the Privacy Act only applies to Medicare, Medicaid, federal institutions, and insurance companies participating through Medicare. Schawbel, *supra* note 3, at 947–48.

Insurance Portability and Accountability Act[105] (HIPAA) and the Health Information Technology for Economic and Clinical Health Act[106] (HITECH Act). The two relevant federal regulations are the Privacy Rule[107] and the Security Rule,[108] both promulgated pursuant to HIPAA.

To briefly summarize this statutory and regulatory regime, HIPAA and the Privacy Rule require HIPAA-covered entities, defined as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form, to comply with federal privacy provisions regarding the disclosure of protected health information.[109] The applicable regulations define protected health information as "[i]ndividually identifiable health information,"[110] which is further defined as information that:

> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
>
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
>
> (i) That identifies the individual; or
>
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[111]

The Privacy Rule requires covered entities to take the following actions with regard to protected health information:

> (1) Provide individuals with notice and certain rights regarding their protected health information;

---

105. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.).

106. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111–5, 123 Stat. 115 (2011).

107. Public Welfare Security and Privacy, 45 C.F.R. pts. 160, 164 (2010).

108. *Id.* pt. 164.

109. *Id.* §§ 160.102–.103. The entities covered by HIPAA and the Privacy Rule will soon expand to include business associates of covered entities pending an upcoming Final Rule from HHS. *See* Modifications to HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40,869 (July 14, 2010) (to be codified at 45 C.F.R. pts. 160, 164) (addressing the expansion of HIPAA restrictions to business associates of covered entities).

110. 45 C.F.R. § 160.103.

111. *Id.*

> (2) Limit the use and disclosure of protected health information;
>
> (3) Obtain authorization from an individual to use or disclose protected health information;
>
> (4) Contract with service providers to provide assurances regarding proper use, appropriate disclosure and appropriate safeguards;
>
> (5) Implement policies and procedures to protect protected health information including: appointing a privacy officer, training the Business Associate's workforce, implementing safeguards and a complaint process.[112]

The Privacy Rule also permits limited uses and disclosures of protected health information, including disclosures to the patient and disclosures and uses related to payment, treatment, and health care operations.[113]

The HITECH Act recently amended HIPAA in several ways relevant to this Article. First, under the HITECH Act, covered entities are required to notify affected persons and HHS when a breach or unauthorized disclosure of unsecured protected health information occurs.[114] Unsecured protected health information includes all information that has not been rendered "unusable, unreadable, or indecipherable to unauthorized individuals," either through encryption or destruction.[115]

Second, business associates of covered entities are now directly required to comply with HIPAA's privacy and security requirements.[116] Third, patients may require that a covered entity not share the patient's protected health information with a health care plan if that person is paying for the health care service in full.[117] Fourth, when disclosing protected health information, the covered entity must disclose only "the minimum necessary" information needed to be disclosed to accomplish the purpose of

---

112. Rebecca Eisner & Mark A. Oram, *Clear Skies or Stormy Weather for Cloud Computing? Critical Privacy and Security Contracting Issues for Customers of Cloud Computing*, 1018 PLI/PAT 409, 427 (2010) (citing 45 C.F.R. pts. 160, 164) (summarizing the HIPAA Privacy Rule standards).

113. 45 C.F.R. § 164.502(a).

114. 42 U.S.C. § 17932 (2006).

115. 45 C.F.R. § 164.402(2)(iii); Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, 74 Fed. Reg. 19,006, 19,006–08 (Apr. 27, 2009) (to be codified at 45 C.F.R. pts. 160, 164).

116. 42 U.S.C. §§ 17931, 17934.

117. *Id.* § 17935(a).

the disclosure.[118] Fifth, patients may request accountings of disclosure of their electronic protected health information over the three-year period prior to the request.[119] Sixth, covered entities and business associates are prohibited from selling protected health information without patient authorization, except under certain circumstances.[120] Seventh, the HITECH Act includes new restrictions on marketing and fundraising and allows patients to opt out of receiving fundraising communications from a covered entity.[121]

Pursuant to the HITECH Act, HHS has issued a Notice of Proposed Rulemaking implementing the HITECH Act HIPAA modifications.[122] The Proposed Rule outlines the following proposed changes:

- Making the Privacy and Security Rules directly applicable to business associates
- Placing new restrictions on the use and disclosure of PHI for marketing and fundraising purposes
- Restricting disclosure of PHI to health plans
- Expanding HIPAA's enforcement of privacy and security provisions
- Amending the definition of business associates.[123]

Given the focus of this Article on the use of encrypted or de-identified patient prescription PHI, two particular provisions of the federal privacy statutes and regulations deserve additional discussion. First, pursuant to the Privacy Rule, a covered entity's use of de-identified patient prescription PHI is considered to be outside the scope of HIPAA and open to dissemination without restriction.[124] The Privacy Rule defines de-identified PHI as PHI for which "seventeen specific fields of data are removed or

---

118. *Id.* § 17935(b).

119. *Id.* § 17935(c).

120. *Id.* § 17935(d).

121. *Id.* § 17936.

122. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40,868 (July 14, 2010) (to be codified at 45 C.F.R. pts. 160, 164).

123. HEATHER DELGADO, UNDERSTANDING HIPAA: A CONTINUING TRANSFORMATION 1–2 (2010) (outlining the most recent legislative and regulatory changes to HIPAA).

124. Gellman, *supra* note 16, at 38 (critiquing HIPAA's assumption that data de-identified in accordance with HIPAA's requirements ensures complete anonymity).

generalized."[125] The Privacy Rule also provides that PHI is only de-identified if "[t]he 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."[126] In sum, HIPAA and the Privacy Rule give short shrift to de-identified health information.

Second, pursuant to the Security Rule, the encryption process for encrypting prescription PHI is defined as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."[127] HHS considers encrypted PHI to be "unusable, unreadable, or indecipherable to unauthorized individuals."[128] In other words, encrypted prescription PHI is considered to be secured PHI, and use of encryption creates "a safe harbor [for covered entities and business associates] to avoid liability for the unauthorized disclosure of protected health information."[129] As with the Privacy Rule and de-identified health information, the Security Rule also fails to provide strong protection for the privacy of encrypted health information.

2. Federal Constitutional Privacy Protections

The foundation for a constitutional right to privacy in health information originally came from Justice Brandeis's dissent in *Olmstead v. United States.*[130] In *Olmstead*, Justice Brandeis asserted the existence of a broad privacy right guaranteed by certain constitutional amendments.[131] In his dissent, Justice Brandeis incorporated the privacy concepts from his law review article almost forty years earlier, stating that these constitutional amendments "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[132]

---

125. *Id.* at 38 (citing 45 C.F.R. § 164.514(b)(2)(i) (2010)).

126. 45 C.F.R. § 164.514(b)(2)(ii).

127. *Id.* § 164.304.

128. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, 74 Fed. Reg. 19,006, 19,006–08 (Apr. 27, 2009) (to be codified at 45 C.F.R. pts. 160, 164).

129. CHERYL S. CAMIN, UPDATING HIPAA COMPLIANCE MEASURES: ADVICE FOR LAWYERS AND THEIR CLIENTS 5 (2010) (addressing the impact of HITECH on HIPAA compliance procedures).

130. Olmstead v. United States, 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting) (disagreeing with the majority that evidence obtained from wiretapping should be suppressed as being obtained in violation of the defendants' Fourth and Fifth Amendment rights).

131. *Id.* at 478.

132. *Id.*

Of course, Justice Brandeis's statement on a constitutional right to privacy was merely the beginning of constitutional privacy jurisprudence. The first Supreme Court precedent acknowledging a right to health-related privacy arose almost forty years later, when *Griswold v. Connecticut* held that state laws prohibiting the use of contraceptives violated a constitutionally based right to marital privacy.[133] Justice Douglas, on behalf of the majority, ruled that a right to marital privacy is grounded within "specific guarantees in the Bill of Rights [that] have penumbras, formed by emanations from those guarantees that help give them life and substance," and that "create zones of privacy."[134]

Following *Griswold*, the Supreme Court expanded its right to privacy jurisprudence further into the health care arena in *Roe v. Wade*.[135] In *Roe*, Justice Blackmun, on behalf of the majority, ruled that the right to privacy is "founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action . . . [and] is broad enough to encompass a woman's decision whether or not to terminate her pregnancy."[136]

While *Roe* focused on decisional privacy or the right to make certain personal decisions without government interference,[137] this Article focuses more on "disclosure privacy" or an individual's constitutional right to control the disclosure of his or her medical information.[138] The Supreme Court's first foray into "disclosure privacy" and medical information privacy was the 1977 case *Whalen v. Roe*.[139] In *Whalen*, Justice Stevens, on behalf of the majority, upheld the constitutionality of a New York statute that required the maintenance of a state-controlled centralized computer file with "the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there is both a lawful and

133. Griswold v. Connecticut, 381 U.S. 479, 484–86 (1965).

134. *Id.* at 484; Mowery, *supra* note 2, at 702 (stating that the Supreme Court has determined that the right to privacy is based on the First, Fourth, Fifth, and Ninth Amendments, and the Fourteenth Amendment's guarantee of liberty).

135. Roe v. Wade, 410 U.S. 113, 153–54 (1973) (holding that Texas criminal abortion laws prohibiting abortions at any stage of pregnancy are unconstitutional).

136. *Id.* at 153.

137. Schawbel, *supra* note 3, at 941–42 (describing the different aspects of the constitutional right to privacy).

138. Whalen v. Roe, 429 U.S. 589, 598–600 (1977) (explaining the two different types of constitutional privacy interests); Schawbel, *supra* note 3, at 941–42 (explaining the concept of a constitutional right to "disclosure privacy").

139. *Whalen*, 429 U.S. at 598–600.

an unlawful market."[140] New York had enacted the statute as a way to monitor, investigate, and enforce laws against prescription drug abuse.[141]

Rejecting the constitutional privacy violation claim, the *Whalen* Court held that the New York statute was unlikely to result in patients refraining from obtaining needed prescription drugs because of the fear of public disclosure.[142] The Court reasoned that the statute was constitutional because "disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient."[143] As further justification for its holding, the Court also recognized that the state has broad police powers in regulating the prescription of drugs.[144]

In the end, the *Whalen* Court ruled that any possible statutory-based harm to patient reputation from public disclosure was insufficient to amount to an invasion of a patient's constitutional right to privacy.[145] Nonetheless, the Court also recognized that increased computerization of health information in the future, particularly within centralized databases, would allow easier access to medical records and heighten right-to-privacy concerns.[146]

Whalen was the Supreme Court's last examination of the constitutional right to privacy within the context of PHI, and it left unanswered the question of whether or not patients have a right to privacy in prescription PHI. Since *Whalen*, various lower courts have looked at this issue to some extent, though often in the context of a right to privacy in personal information as opposed to the narrow field of PHI or prescription PHI. Reviewing those cases, "there is an unresolved circuit split as to whether there is a constitutional right to protection against disclosure of personal information."[147] Nine circuits recognize a constitutional right to privacy in personal information, health or otherwise,[148] while the Sixth Circuit has

---

140. *Id.* at 591 (holding that the state's police power justified any privacy invasion resulting from the maintenance of a state-mandated centralized prescription monitoring system).

141. *Id.* at 597–98.

142. *Id.* at 600.

143. *Id.* at 602.

144. *Id.* at 603 n.30.

145. *Id.* at 603–04.

146. *Id.* at 605.

147. Woodage, *supra* note 86, at 688; *see also* Ward, *supra* note 5, at 76 ("Although courts have acknowledged a privacy right exists in pharmaceutical records, the magnitude of this right has not been completely defined." (citing Alison M. Jean, *Personal Health and Medical Information: The Need for More Stringent Constitutional Privacy Protection*, 37 SUFFOLK U. L. REV. 1151, 1153–54 (2004))); Woodage, *supra* note 86, at 688 (noting a circuit split with regard to whether or not the Constitution protects against the disclosure of personal information).

148. Woodage, *supra* note 86, at 688 (citing Diane M. DeGroat, *When Students Test Positive,*

reached the opposite conclusion,[149] and the Eighth Circuit recognizes such a right only in instances involving egregious disclosure.[150]

Drilling down on several of these circuit court rulings, in *Doe v. Southeastern Pennsylvania Transportation Authority (SEPTA)*, the plaintiff, an employee of SEPTA, filed a section 1983 civil rights claim against his supervisor and SEPTA for invasion of privacy after they discovered, through a review of his prescription records, that he suffered from HIV.[151] The Third Circuit held that the employee had a constitutional right to privacy in his prescription drug records, but that his right to privacy was not absolute and was subject to intermediate scrutiny as to whether the employer's interest in obtaining the records outweighed the employee's privacy interest in those records.[152] The court held that SEPTA's interest in monitoring its prescription drug program for fraud and abuse outweighed the plaintiff's privacy interest in his prescription drug records.[153] The court characterized the employer's privacy intrusion to be minimal and held that SEPTA did not need to prove that it had a compelling interest in obtaining the prescription information.[154]

Similarly, in *Douglas v. Dobbs*, the Tenth Circuit ruled that individuals have a non-absolute right to privacy within their prescription drug records and that state laws may operate to diminish one's expectation of privacy in those records.[155] The *Douglas* court followed *Whalen* in finding that the government has broad police powers to justify regulation of the prescription

---

Their Privacy Fails: The Unconstitutionality of South Carolina's HIV/AIDS Reporting Requirement, 17 AM. U. J. GENDER SOC. POL'Y & L. 751, 761 (2009)); *see also* Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); Daury v. Smith, 842 F.2d 9, 13 (1st Cir. 1988); Fadjo v. Coon, 633 F.2d 1172, 1175 (5th Cir. 1981) (collectively recognizing a constitutional right to privacy in personal information).

149. Woodage, *supra* note 86, at 688 (citing Doe v. Wigginton, 21 F.3d 733, 740 (6th Cir. 1994)).

150. *Id.* (citing Alexander v. Peffer, 993 F.2d 1348, 1350 (8th Cir. 1993)).

151. Doe v. Se. Penn. Transp. Auth. (SEPTA), 72 F.3d 1133, 1134–35 (3d Cir. 1995) (holding that SEPTA's need for access to plaintiff's prescription records for insurance plan monitoring purposes outweighed plaintiff's privacy interest in those records).

152. *Id.* at 1139–40 (holding that an intermediate scrutiny analysis applies and not a compelling interest analysis because the latter only applies when the degree of intrusion into individual privacy is severe).

153. *Id.* at 1140, 1142–43 (applying the *United States v. Westinghouse Electric Corp.*, 638 F.2d 570 (3d Cir. 1980), balancing test for determining the constitutionality of a privacy intrusion by balancing the interest in public disclosure against the privacy interest, and holding "that a self-insured employer's need for access to employee prescription records under its health insurance plan, when the information disclosed is only for the purpose of monitoring the plans by those with a need to know, outweighs an employee's interest in keeping his prescription drug purchases confidential").

154. *Id.* at 1139–40, 1143.

155. Douglas v. Dobbs, 419 F.3d 1097, 1102 (10th Cir. 2005) (holding that an assistant district attorney in a civil rights action was entitled to qualified immunity for approving a law enforcement request to search a patient's pharmacy records for evidence of abuse of pain medication).

of drugs and certain privacy invasions regarding prescription drug records.[156]

Rounding out this trio of cases, in *United States v. Sutherland*, federal prosecutors sought to compel production of patient pharmacy records from a hospital in connection with the prosecution of a physician for unlawful distribution and dispensing of controlled substances.[157] Following *Whalen* and *SEPTA*, the Tenth Circuit held that a patient's right to privacy in prescription records is not absolute and must be balanced against the government's need for those records.[158] The court found that the federal prosecutors had a compelling interest in the production of the patient prescription records, but also held that patients should have the opportunity to object to the production of their records in light of the strong federal policy protecting the privacy of patient health information.[159]

As demonstrated by these cases and the circuit court split, the strength of a constitutional right to privacy in prescription PHI, including de-identified prescription PHI, and what sort of constitutional scrutiny is applied to burdens upon such a right are still somewhat open questions.[160] As the Third Circuit recently observed, "the question of the scope of the constitutional right to privacy in one's medical information is largely unresolved."[161] Such uncertainty and unresolved constitutional questions further demonstrate the need for uniform federal legislation protecting a patient's privacy right in both identifiable and de-identified prescription PHI.

C. State Legislative Responses to Data Mining and Detailing

Along with the broad-based state and federal privacy-protection options outlined above, the most recent direct attempt at regulating the use of prescription data involved three state statutes that focused on regulating data mining and detailing. Over approximately the past five years, New Hampshire, Vermont, and Maine each enacted statutes directed toward

---

156. *Id.* at 1102 n.3.

157. United States v. Sutherland, 143 F. Supp. 2d 609, 610 (W.D. Va. 2001).

158. *Id.* at 611–12 (citing Whalen v. Roe, 429 U.S. 589, 602 (1977); *SEPTA*, 72 F.3d at 1138 (holding that a hospital could not produce patients' pharmacy records at trial without giving patients an opportunity to object); Ward, *supra* note 5, at 76 (noting that "the American legal system has long recognized that an individual's right to privacy must be balanced with the state's ability to exercise its police power" and protect public welfare).

159. *Sutherland*, 143 F. Supp. 2d at 613.

160. Han, *supra* note 2, at 136 (stating that courts will be asked in the future to determine what is required to protect patient privacy rights in prescription records).

161. Citizens for Health v. Leavitt, 428 F.3d 167, 177 n.10 (3d Cir. 2005) (holding that the HIPAA Privacy Rule did not infringe on patients' right to privacy in their personal health information).

curtailing data mining of prescription information and the use of that information for detailing purposes. Despite indirectly protecting, to some extent, patient privacy in prescription PHI, these state statutes were targeted more at regulating data mining and detailing from the prescriber's perspective rather than from the patient privacy perspective.

1. New Hampshire

The first legislative effort to restrict the data mining of prescription information was New Hampshire's 2006 Prescription Information Law (PIL), which prohibited the license, transfer, use, or sale of patient-identifiable and prescriber-identifiable prescription information for certain commercial purposes.[162] Those commercial purposes included "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."[163] New Hampshire sought to ensure compliance with PIL through various civil and criminal penalties, including subjecting violators to possible misdemeanor or felony prosecution,[164] civil monetary penalties of up to $5,000 per violation,[165] and misdemeanor or felony prosecution under New Hampshire's unfair and deceptive trade practices law.[166]

---

162. N.H. REV. STAT. ANN. § 318:47-f (2011).

> Records 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, except for the limited purposes of 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. 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.

Id. § 318-B12(IV).

163. *Id.* § 318-B12(IV).

164. *Id.* § 318:55.

165. *Id.*

166. *Id.* §§ 318:47-f, 358-A:2, 358-A:6.

2. Vermont

Following New Hampshire's passage of PIL, Vermont enacted a modified opt-in version of the New Hampshire law in 2007.[167] In relevant part, the Vermont law provided that a pharmaceutical manufacturer, a pharmaceutical marketer, "an electronic transmission intermediary, a pharmacy, or other similar entity shall 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."[168] The statute defined the term "marketing" to:

> include advertising, promotion, or any activity that is intended to be used or is used to influence sales or the market share of a prescription drug, influence or evaluate the prescribing behavior of an individual health care professional to promote a prescription drug, market prescription drugs to patients, or evaluate the effectiveness of a professional pharmaceutical detailing sales force.[169]

The statute essentially prohibited using prescriber-identifiable information for marketing purposes, unless the prescriber agreed to or opted in to such a use. A prescriber would opt in through his or her licensing applications or renewal forms and could revoke his or her opt-in at any time.[170]

Along with its substantive provisions and procedural requirements, the Vermont law also provided for an enforcement scheme for violations. With regard to violations of the law, the statute provided for the application of any remedy provided by law, as well as for a cause of action on behalf of the Attorney General of Vermont, which would be akin to a civil claim under Vermont's Consumer Fraud Act.[171]

3. Maine

The third state to target prescription data mining and detailing was Maine, which, in 2008, enacted an opt-out prescription drug information

---

167. IMS Health Inc. v. Sorrell, 630 F.3d 263, 269 (2d Cir. 2010).
168. VT. STAT. ANN. tit. 18, § 4631(d) (West 2011).
169. *Id.* § 4631(b)(5).
170. *Id.* § 4631(c)(1).
171. *Id.* § 4631(f).

confidentiality law.[172] Unlike the Vermont approach, which prohibited marketing with the use of prescriber data unless the prescriber consented, the Maine approach allowed marketing with the use of prescriber data unless the prescriber opted for confidentiality protection.

The Maine law provided an option for Maine prescribers, as part of their application for licensure or re-licensure, to protect the confidentiality of their identifying information in prescriptions when such information would otherwise be "used for marketing purposes by carriers, pharmacies and prescription drug information intermediaries."[173] The Maine statute defined "marketing" as:

> (1) Advertising, publicizing, promoting or selling a prescription drug;
>
> (2) Activities undertaken for the purpose of influencing the market share of a prescription drug or the prescribing patterns of a prescriber, a detailing visit or a personal appearance;
>
> (3) Activities undertaken to evaluate or improve the effectiveness of a professional detailing sales force; or
>
> (4) A brochure, media advertisement or announcement, poster or free sample of a prescription drug.[174]

Under the Maine statute, if a prescriber were to opt-out, then a carrier or prescription drug information intermediary would not be allowed to "license, use, sell, transfer or exchange for value, for any marketing purpose, prescription drug information that identifies directly or indirectly the individual."[175] The data miners and pharmaceutical companies were notified of the opted-out prescribers through public monthly updated lists "of all prescribers who have filed with the licensing board for confidentiality protection."[176] Maine sought to enforce the statute by authorizing a civil cause of action for damages under the Maine Unfair Trade Practices Act.[177]

---

172. ME. REV. STAT. ANN. tit. 22, § 1711-E (2011).
173. *Id.* § 4-A.
174. *Id.* § 1-F-1.
175. *Id.* § 2.
176. *Id.* § 4-A-2.
177. *Id.* § 3.

D. The Data-Mining Court Cases

As may be expected, all three of the state statutes outlined above have since been challenged in federal court on constitutional grounds, resulting in three circuit court decisions and, ultimately, a Supreme Court decision on the constitutionality of the Vermont statute. Perhaps reflecting the prescriber-centric focus of the statutes being challenged, all three of the circuit court decisions, as well as the Supreme Court decision, focused more on data mining and detailing from the prescriber privacy perspective than from the patient privacy perspective. Nonetheless, these cases highlight some of the important constitutional concerns that arise when crafting or analyzing alternatives for protecting the privacy of patient prescription PHI. Moreover, the Supreme Court decision provides guidance as to how to craft a legislative proposal to protect the privacy of patient prescription PHI that will likely pass constitutional muster.

1. *IMS Health Inc. v. Ayotte*

The first circuit court decision to address the New England data mining statutes was *IMS Health Inc. v. Ayotte*, which arose out of two data-mining companies' challenge to the New Hampshire PIL on grounds that the law infringed upon their free speech and violated the Commerce Clause.[178] In *Ayotte*, a split panel of the First Circuit held that PIL regulated conduct and not speech, thereby garnering lax constitutional scrutiny.[179] The court ruled that PIL regulated conduct because PIL's regulation of prescription data was essentially a regulation on data as a commodity, like beef jerky, not data as a form of speech.[180]

The court further held that to the extent that PIL regulated speech, it regulated commercial speech, requiring more lax constitutional scrutiny than core First Amendment speech.[181] Accordingly, the Court applied the *Central Hudson*[182] test for commercial speech, which provides that government restrictions on commercial speech are permissible if they

178. IMS Health Inc. v. Ayotte, 550 F.3d 42, 47–48 (1st Cir. 2008) (upholding the constitutionality of the New Hampshire data-mining statute on the grounds that it regulated conduct and not speech).

179. *Id.* at 52.

180. *Id.* at 53.

181. *Id.* at 54–55.

182. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 564–66 (1980) (outlining the Supreme Court's test for determining the constitutionality of regulations on commercial speech).

directly advance a substantial governmental interest and restrict speech no more than is necessary to further that interest.[183]

Applying the *Central Hudson* test, the court ruled that the PIL goal of containing health care costs was a substantial governmental interest.[184] The court also held that PIL directly advanced that governmental interest because the evidence demonstrated that detailing increases the cost of prescription drugs, that prescriber histories improve the success of detailing, and that despite the increased costs, "detailing does not contribute to improved patients' health."[185] In reaching this conclusion, the court deferred heavily to legislative judgment regarding the health impacts and costs of detailing, particularly given that New Hampshire was a trailblazer and "the first state to deny detailers access to prescribing histories."[186]

Moving to the third prong of the *Central Hudson* test, the court ruled that there existed no alternative legislative approaches that would have achieved the goals of PIL without restricting speech.[187] Rejecting other possible alternatives as harmful or ineffective, the court ruled that banning free drug samples would harm indigent patients; the state would be unable to spend enough money to engage in an effective counter-detailing education campaign of prescribers with regard to generic drugs; and requiring physicians to consult with pharmacists before brand-name drugs could be prescribed in favor of non-bioequivalent generic substitutes would ineffectively focus on the process after the detailing has already occurred.[188]

Having resolved the First Amendment speech issue, the court's final ruling addressed the data miners' claim that PIL violated the dormant Commerce Clause because it failed to include a geographic limitation and directly regulated out-of-state transactions between data miners selling prescription data to pharmaceutical manufacturers.[189] The court rejected this argument, presuming instead that PIL governed only in-state conduct and domestic transactions, even though it "may result in a loss of profit to out-of-state data miners due to the closing of one aspect of the New Hampshire market for their wares."[190]

While the *Ayotte* case fully explored the speech implications and Commerce Clause implications of PIL, the *Ayotte* court notably avoided any detailed discussion of patient privacy interests within the context of

183. *Ayotte*, 550 F.3d at 55.
184. *Id.*
185. *Id.* at 55–56.
186. *Id.* at 58.
187. *Id.* at 60.
188. *Id.* at 59–60.
189. *Id.* at 63.
190. *Id.* at 64.

PIL. Rather, the court merely acknowledged, with regard to the *Central Hudson* test, that New Hampshire asserted patient privacy as a substantial governmental interest advanced by PIL.[191] Similarly, the concurring and dissenting opinions avoided discussing patient privacy implications of PIL, reasoning that such a discussion would be moot because the plaintiffs did not challenge the statute's restriction on the use of patient-identifiable prescription information.[192]

2. *IMS Health Inc. v. Mills*

The First Circuit revisited the *Ayotte* decision in a similar ruling with regard to three data miners' challenge to the Maine prescriber confidentiality law.[193] Finding the nature of the suit and the Maine statute to be very similar to those at issue in *Ayotte*, the court relied upon *Ayotte* in holding that the Maine "statute regulates conduct, not speech, and even if it regulates commercial speech, [the statute] satisfies constitutional standards."[194]

Despite finding that the Maine law regulated conduct and not speech, the *Mills* court, like the *Ayotte* court, still went through the exercise of applying the *Central Hudson* test, ruling that through its opt-in provision, the Maine law "directly advances the substantial purpose of protecting opted-in prescribers from having their identifying data used in unwanted solicitations by detailers, and thus Maine's interests in lowering health care costs."[195] The court likened the statute to a "do not call" or "do not mail" list, which have been held to be constitutional and which protect a listener's right to be left alone.[196]

Turning to the second and third *Central Hudson* prongs, the court ruled that the evidence established that Maine prescribers had complained and objected to detailing and detailers' use of personal identifying prescribing histories, and that the Maine law would directly advance the state's interest in protecting against these harms.[197] Moreover, the court ruled that the Maine law's opt-in mechanism, by definition, was a least restrictive means

---

191. *Id.* at 55.

192. *Id.* at 80 n.42, 85 (Lipez, J., concurring and dissenting).

193. IMS Health Inc. v. Mills, 616 F.3d 7, 13 (1st Cir. 2010) (upholding the constitutionality of the Maine data-mining statute on the grounds that the statute regulated conduct and not speech).

194. *Id.*

195. *Id.* at 19.

196. *Id.* at 21–22 (citing Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 736–38 (1970); FTC v. Mainstream Mktg. Servs., Inc., 345 F.3d 850, 854–55 (10th Cir. 2003)).

197. *Id.* at 22.

of protecting prescribers' privacy interests.[198] Instead of the government identifying a given type of speech as harmful, the Maine law was an effort by the government to empower prescribers to regulate when they deemed data-miner speech to be harmful.[199]

Examining the Commerce Clause challenge, the court ruled that the Maine statute survived constitutional scrutiny because the regulation of data miners' out-of-state transactions involving prescription data was "a necessary incident of Maine's strong interest in protecting opted-in Maine prescribers from unwanted solicitations, a policy that Maine also rationally believes will lower its health care costs."[200] The court reasoned that Maine was attempting to regulate extraterritorial conduct with a substantial in-state impact, and that even though the Maine law regulated extraterritorial conduct, the regulation did not "discriminate against out-of-state entities in favor of in-state competitors . . . [and did] not risk imposing regulatory obligations inconsistent with those of other states."[201]

The court also ruled that the data miners failed to demonstrate a disproportionate burden on interstate commerce in relation to the in-state benefits conferred under the Maine law.[202] The court held that Maine was able to demonstrate that the law created substantial in-state benefits for Maine prescribers who wanted to avoid unwanted targeting.[203] On the other side of the ledger, the court reasoned that the data miners' loss of a portion of the Maine market would not seriously impact their products' marketability and that the cost to data miners of complying with the Maine law would prove insubstantial, given that they needed only to ensure that they avoid using or selling opted-in Maine prescriber data.[204]

As in the *Ayotte* case, despite addressing the speech and Commerce Clause aspects of the Maine law, the *Mills* majority and concurrence did not substantively address the patient privacy implications of the Maine statute. The majority opinion did not address the issue at all, and the concurring opinion merely referenced the fact that Maine asserted patient privacy as a substantial governmental interest, justifying any statutory burden on commercial speech.[205]

---

198. *Id.*
199. *Id.*
200. *Id.* at 14.
201. *Id.* at 26, 28.
202. *Id.* at 32.
203. *Id.*
204. *Id.*
205. *Id.* at 36 (Lipez, J., concurring).

3. *IMS Health Inc. v. Sorrell*

The third circuit court case in the trio of cases challenging the state data-mining statutes was *IMS Health Inc. v. Sorrell*, in which data miners and the Pharmaceutical Research Manufacturers of America (PhRMA), an association of pharmaceutical manufacturers, challenged the constitutionality of the Vermont data-mining statute.[206] Starting with the speech-versus-conduct issue, the Second Circuit criticized the *Ayotte* decision for creating a false distinction between data as an informational asset, akin to a commercial product, and speech.[207] The court ruled that the Vermont statute plainly regulated speech, given that it aimed to alter the information provided to prescribers through detailing, thereby intending to influence the supply of information.[208] The court further emphasized that the statute "prevents willing sellers and willing buyers from completing a sale of information to be used for purposes that the state disapproves."[209]

The court concluded that the Vermont statute regulated commercial speech and therefore analyzed the statute under the *Central Hudson* test.[210] The court ruled that the aim of the statute to protect the privacy of prescribers was not a substantial state interest because the statute banned only certain uses of prescription data, thereby allowing prescription data to be distributed for any other purpose besides the prohibited purpose.[211] The court also held that the asserted state interest in prescriber privacy was too speculative because Vermont was unable to demonstrate that the regulation of prescription data impacted the privacy of the doctor–patient relationship and "the integrity of the prescribing process or the trust patients have in their doctors."[212] Nonetheless, the court ruled that Vermont did have a substantial interest in lowering health care costs and protecting the public health, which the statute purported to promote.[213]

Focusing on whether the Vermont statute directly advanced the state interest in reducing health care costs and protecting public health, the court held that the statute only indirectly promoted these interests because it failed to directly restrict prescribing practices or restrict detailers'

---

206. IMS Health Inc. v. Sorrell, 630 F.3d 263, 266–67 (2d Cir. 2010) (holding that the Vermont statue abridged the data miners' commercial speech rights because it did not directly advance the state's asserted interests and was not narrowly tailored to serve those interests).

207. *Id.* at 272.

208. *Id.*

209. *Id.* at 273.

210. *Id.* at 275.

211. *Id.* at 275–76.

212. *Id.* at 276.

213. *Id.*

marketing practices.[214] Instead, the statute directly regulated the transfer of prescription data from data miners to pharmaceutical manufacturers, which only indirectly impacted prescriber and detailer behavior and the goals of cost containment and promotion of public health.[215] The court explained that courts should be skeptical of government regulations on the dissemination of information in order to alter an individual's conduct, which is what the Vermont statute did by limiting the type of information available to prescribers in order to impact their prescribing behavior.[216]

Along with finding that the Vermont statute failed to survive intermediate scrutiny under the *Central Hudson* test, the court also ruled that the state's purported interests could have been fulfilled in a less speech-restrictive manner.[217] The Vermont statute was overly burdensome because it promoted fewer prescriptions of all brand-name drugs. This was a poor fit with the legislative goal of restricting the over-prescription of only "new and allegedly insufficiently tested brand-name drugs in cases where there are cheaper generic alternatives available."[218] The court found that Vermont could have achieved its goal by funding its own prescriber education program to counter the detailers' speech or by mandating "the use of generic drugs as a first course of treatment, absent a physician's determination otherwise."[219] The court faulted the state for failing to produce arguments or evidence for why the proposed alternatives would have been inadequate to serve the state's goals.[220]

Unlike the *Ayotte* and *Mills* cases, the *Sorrell* case did address the patient privacy implications of the Vermont statute. The court specifically held that the state's interest in medical privacy, including patient trust in their physicians and the integrity of the prescribing process, was too speculative to serve as a substantial governmental interest to justify the state's regulation on commercial speech.[221] The dissent, on the other hand, opined that patient privacy was a substantial governmental interest worthy of protection under the Vermont statute.[222] In support of its position, the dissent highlighted the importance placed on patient privacy by federal legislation, such as HIPAA, and the goal of such legislation to prevent

---

214. *Id.* at 277.
215. *Id.*
216. *Id.* at 277–78.
217. *Id.* at 279.
218. *Id.*
219. *Id.* at 280.
220. *Id*. at 281.
221. *Id.* at 276.
222. *Id.* at 290 (Livingston, J., dissenting).

"rampant dissemination of confidential information."[223] The dissent opined that the Vermont statute both substantially furthered the state's interest in medical privacy and was narrowly tailored to such an end.[224]

4. *Sorrell v. IMS Health Inc.*: The Supreme Court Decision

Following *Ayotte*, *Mills*, and *Sorrell*, the Supreme Court resolved the circuit split and issued the final word on the New England data-mining statutes by affirming the *Sorrell* decision and finding the Vermont statute unconstitutional.[225] First, addressing the speech-versus-conduct question, the Court found the Vermont statute to be a content-based, speaker-based, and viewpoint-based restriction on the sale, disclosure, and use of prescriber-identifying information.[226] The Court explained that the Vermont law prevented detailers, and only detailers, from communicating with prescribers, and did so because the State disagreed with the message that the detailers were conveying to prescribers.[227] Accordingly, the Court applied heightened scrutiny to the Vermont law, holding that the commercial nature of the speech at issue did not reduce the level of scrutiny to be applied because the Vermont law targeted a specific viewpoint.[228]

In finding the Vermont statute to be a regulation of speech entitled to heightened scrutiny, the Court also rejected the beef jerky/commodity argument from *Ayotte*.[229] The Court ruled that prescriber-identifying information is not merely data like a commodity but rather comprises facts that form the foundation for speech and communication.[230] Therefore, restricting or prohibiting use of facts essential for communication is no different than prohibiting the communication itself. The Court likened the situation as being no different than "a law prohibiting trade magazines from purchasing or using ink."[231]

Although the Court held that the Vermont statute was entitled to heightened scrutiny, the Court alternatively applied the *Central Hudson* test for commercial speech.[232] First, the Court rejected Vermont's argument that

---

223. *Id.* at 291.

224. *Id.* at 293–97.

225. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2659 (2011).

226. *Id.* at 2663.

227. *Id.*

228. *Id.* at 2664 (holding that "[t]he First Amendment requires heightened scrutiny whenever the government creates 'a regulation of speech because of disagreement with the message it conveys'" (quoting Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989))).

229. *Id.* at 2667.

230. *Id.*

231. *Id.*

232. *Id.* at 2667–68.

the statute fulfilled prescribers' expectation that their prescriber-identifying information would only be used for filling and processing prescriptions.[233] The Court explained that the Vermont statute did not serve this interest because it allowed prescriber-identifying information to be used for a host of reasons with only one exception—the information could not be used for marketing.[234] In providing this rationale, the Court notably implied that a different result might occur if the State were to advance "its asserted [prescriber] privacy interest by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances."[235]

Second, the Court rejected Vermont's argument that the statute's prescriber opt-in provision saved the statute from being overly burdensome of speech.[236] Though opt-in measures in the hands of private decision-makers can insulate government-imposed statutory burdens on speech from First Amendment scrutiny, the Court noted that the Vermont statute conditioned prescribers' access to privacy protection on acquiescence "in the State's goal of burdening disfavored speech by disfavored speakers."[237] In other words, the statute allowed prescribers to maintain the privacy of their prescriber-identifying information, but only if they agreed to limit access to such information with regard to detailers, and only detailers, which the State disfavors. The Court seemed to imply that if the choice on the scope of privacy options available to prescribers through opting in were more unfettered or unlimited, then the opt-in provision might more effectively insulate the statute from First Amendment challenge.[238]

Third, the Court rejected the State's claim that the statute protects the government's interest in protecting doctors from harassing sales behaviors.[239] The Court doubted whether a few physicians feeling harassed could justify the statute's content-based restriction on speech and noted that the State failed to explain why other remedies might not equally address this harassment concern.[240]

Fourth, the Court rejected Vermont's claim "that detailers' use of prescriber-identifying information undermines the doctor–patient

---

233. *Id.* at 2668.

234. *Id.*

235. *Id.*

236. *Id.* at 2669 (explaining that the opt-in provision "may offer a limited degree of privacy, but only on terms favorable to the speech the State prefers").

237. *Id.*

238. *Id.* (holding that "[r]ules that burden protected expression may not be sustained when the options provided by the State are too narrow to advance legitimate interests or too broad to protect speech").

239. *Id.* at 2669–70.

240. *Id.* at 2669.

relationship by allowing detailers to influence treatment decisions."[241] The Court reasoned that Vermont failed to explain why other uses of prescriber-identifying information would not equally undermine the doctor–patient relationship.[242] Moreover, the Court found that Vermont's justification turns the First Amendment on its head because it bases the State's power to burden speech on the fear that the speech might persuade or influence prescriber prescription decisions.[243]

Fifth, the Court rejected the State's claim that the statute promoted lower medical costs and better public health by advancing low cost, safer generic drugs over more expensive, less time-tested brand-name drugs.[244] The Court reiterated that the State impermissibly sought to achieve these goals by attempting to reduce the strength of detailers' influence on prescription decisions, thereby decreasing the volume of prescribed brand-name drugs.[245] The Court held that speech that the State finds to be too persuasive against its preferred viewpoint does not justify burdening that speech or the speaker.[246] The Court noted that there is an ongoing debate regarding the safety and effectiveness of brand-name drugs versus generic drugs and that such a debate should be resolved through free and uninhibited speech on both sides of the issue.[247] The State must not burden the speech, but must counter the speech with speech of its own.[248]

In concluding its decision, the Court noted that "[t]he capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure."[249] However, the Court also held that content-based discriminatory approaches to resolving these issues are impermissible and unconstitutional.[250] Still, in providing future guidance to would-be regulators, the Court intimated that "[i]f Vermont's statute provided that prescriber-identifying information

---

241. *Id.* at 2670.

242. *Id.*

243. *Id.* (stating that "[a]bsent circumstances far from those presented here, the fear that speech might persuade provides no lawful basis for quieting it").

244. *Id.*

245. *Id.*

246. *Id.* at 2671 ("The First Amendment directs us to be especially skeptical of regulations that seek to keep people in the dark for what the government perceives to be their own good." (quoting 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 503 (1996))).

247. *Id.*

248. *Id.*

249. *Id.* at 2672.

250. *Id.*

could not be sold or disclosed except in narrow circumstances then the State might have a stronger position."[251]

The Supreme Court's *Sorrell* decision, in effect, renders the New Hampshire and Maine data-mining statutes unconstitutional, as well as the Vermont statute. Though the former two statutes may approach the regulation of data mining and detailing through slightly different methods than the Vermont statute, both statutes plainly discriminate against the content and the viewpoint of detailers and should be held unconstitutional pursuant to *Sorrell*.

Accordingly, the *Sorrell* decision yields two important points in terms of the scope of this Article. First, it teaches that none of the three New England statutes, as they stand, are viable alternatives for protecting the privacy of patient prescription PHI. As such, new pathways to achieve this goal must be considered. Second, and more importantly, the Court's openness to more narrowly tailored means of restricting the use of prescriber-identifying information provides guidance for the creation of a statute that will provide privacy protection for patient prescription PHI in a constitutional manner.[252] The next Part of this Article evaluates the strengths and weaknesses of existing options for protecting the privacy of patient prescription PHI and lays the groundwork for such a statutory proposal.

IV. EVALUATING THE ALTERNATIVES FOR PROTECTING PATIENT PRESCRIPTION INFORMATION PRIVACY

Reviewing federal and state statutes, ethical codes, state common law, and federal constitutional law, there are a number of available options that protect patient prescription information privacy. This Part seeks to examine each option. While some of these options may seem promising, each one suffers from weaknesses that prevent them from being an optimal solution for protecting either identified or de-identified patient prescription PHI.

A. The New England Data-Mining Statutes

As outlined above, the Vermont data-mining statute has been held unconstitutional by the Supreme Court, and that decision extends to the New Hampshire and Maine statutes as well. Accordingly, these statutes are no longer viable options for protecting patient prescription information privacy. Nonetheless, it is important to examine these statutes in order to identify their practical weaknesses. Understanding such weaknesses will

---

251. *Id.*
252. *Id.*

provide guidance for how to formulate a stronger and more constitutionally sound legislative solution for protecting the privacy of patient prescription PHI.

The New Hampshire and Vermont statutes are woefully inadequate in addressing patient privacy interests, particularly privacy interests in de-identified patient prescription PHI. The New Hampshire statute only protects the privacy of patient-identifying information and says nothing about de-identified or encrypted patient information.[253] Whereas the Vermont statute intends to protect the privacy of prescription information,[254] it never mentions a method for protecting patient prescription PHI and focuses entirely on protecting prescriber-identifying information.[255]

In contrast to the New Hampshire and Vermont statutes, the Maine statute comes closest to a meaningful attempt to protect both identified and de-identified or encrypted patient prescription PHI. The Maine statute specifically provides that "[a] carrier or prescription drug information intermediary may not license, use, sell, transfer or exchange for value, for any marketing purpose, prescription drug information that identifies directly or indirectly the [patient]."[256] For patient privacy purposes, the upside of this statutory language is the possibility that the phrase "identifies directly or indirectly" encompasses de-identified and encrypted patient prescription PHI. However, there is no definition of the term "indirectly" within the statute, so there is no definitive answer on this issue.

Even if de-identified or encrypted patient information is protected under the Maine statute, the restriction on sale or transfer of that information narrowly applies only to carriers and drug information intermediaries and only for marketing purposes. This approach was the fatal constitutional weakness for the Vermont statute.[257] Any other individual or entity, including drug manufacturers or researchers, can use prescription information for marketing and other purposes without violating the Maine statute.[258] Under the Maine statute, a pharmacy could lawfully sell or transfer the patient prescription information directly to a pharmaceutical manufacturer for marketing purposes.

---

253. N.H. REV. STAT. ANN. § 318:47-f (2011).

254. VT. STAT. ANN. tit. 18, § 4631(a) (West 2011).

255. *Id.* § 4631.

256. ME. REV. STAT. ANN. tit. 22, §§ 1711-E-2, E-1-F (2011).

257. *Id.* § 1711-E-2, 2-A.

258. IMS Health Inc. v. Mills, 616 F.3d 7, 33 (1st Cir. 2010) (Lipez, J., concurring) (noting that the Maine statue does not actually directly limit drug companies or detailers' marketing efforts using prescriber-identifiable information).

All three of the New England data-mining statutes are simply too narrow in scope to fully protect the privacy of patient prescription PHI. All three proscribe the use of prescription information but only for marketing purposes.[259] While some patients may consider marketing the only use for which they want their prescription information protected, other patients may legitimately want the privacy of their prescription information protected from use in other contexts, such as for research purposes.

Turning to the opt-in and opt-out provisions in the Vermont and Maine statutes, a major concern is that both statutes use opt-in and opt-out lists, which are not real-time lists. For example, the Maine statute only requires monthly updates to the list of prescribers seeking confidentiality protection under the statute.[260] Even worse, in Vermont, entities seeking to use prescriber prescription information need only check the list of prescribers seeking confidentiality protection once every six months.[261] These respective statutory provisions are essentially loopholes that allow for substantial time gaps during which those who wish to access and use prescription information may do so without fear of penalty.

To some extent, the statutory weaknesses outlined above are probably a reflection of the three statutes' primary focus on prescriber privacy and prescriber concerns with data mining and detailing, as opposed to patient concerns.[262] This prescriber-centric focus is most apparent in the opt-in and opt-out provisions of the Vermont and Maine statutes, which empower the prescriber, not the patient, to maintain the confidentiality of prescription information.[263]

Even if the three statutes are sufficiently patient-privacy-centric, they still lack clear, simple, and vigorous compliance and enforcement provisions. Neither the New Hampshire statute nor the Maine statute directly regulates the marketing of prescription information.[264] Rather, the two statutes place the burden on pharmacies, data miners, insurers, and

---

259. ME. REV. STAT. ANN. tit. 22, § 1711-E-2; N.H. REV. STAT. ANN. § 318:47-f (2011); VT. STAT. ANN. tit. 18, § 4631(d).

260. ME. REV. STAT. ANN. tit. 22, § 1711-E-4-A-2.

261. VT. STAT. ANN. tit. 18, § 4631(c)(2).

262. IMS Health Inc. v. Sorrell, 630 F.3d 263, 270 (2d Cir. 2010) (finding the protection of prescriber privacy to be one of the primary legislative purposes for the Vermont statute); *Mills*, 616 F.3d at 12 (finding the purpose of the Maine statute to be protecting prescribers' data privacy); IMS Health Inc. v. Ayotte, 550 F.3d 42, 61 (1st Cir. 2008) (finding the intent of the New Hampshire law to be the prevention of targeted detailing by pharmaceutical companies using prescriber histories).

263. 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).

264. VT. STAT. ANN. tit. 18, § 4631(d); *Mills*, 616 F.3d at 33 n.37 (Lipez, J., concurring) (noting that the Maine statute "also bars pharmaceutical manufacturers and marketers from using the information for marketing or promoting a prescription drug unless the prescriber consents").

similar entities not to transfer the prescription information to downstream marketers for marketing purposes.[265] This creates a bizarre enforcement mechanism. As the *Mills* concurring opinion noted, this enforcement structure forces the pharmacies, data miners, insurers, and like entities to police their own customers.[266] How the state would discover violations and enforce the prohibition against downstream marketing is also far from clear.[267]

When statutory violations occur under the three statutes, it is also unclear how patients will become aware that their prescription information is being used in an unlawful manner. There may be some obvious violations, such as where a patient uses "Drug X" and then receives direct marketing materials to encourage the use of Drug X, or direct marketing materials that reference Drug X and solicit a switch to a similar competitor drug. A patient rightfully might be suspicious of such practices. However, in terms of compliance and enforcement, of greater and more likely concern are situations in which drug manufacturers engage in direct advertising to patients, using patient prescription information in a manner that does not raise red flags. Effective marketers will learn how to directly market to a patient using that patient's prescription information, but in such a way that the patient cannot tell whether the drug manufacturer used that information to target or solicit him or her.

There is simply insufficient transparency within the New England data-mining statutes to raise awareness of possible statutory violations. Reviewing the three state statutes, it is unclear how state enforcement agencies, prescribers, and especially patients would become aware of breaches of prescription information privacy. There is nothing within the state statutes that requires pharmaceutical manufacturers to publish to the world how they design their marketing campaigns or what information they use to design them. While the statutory penalties may nonetheless promote deterrence, potential data-miner and drug-manufacturer violators may soon discover that it will be difficult for patients, prescribers, or the states to discover such violations.

---

265. N.H. REV. STAT. ANN. § 318:47-f (2011); ME. REV. STAT. ANN. tit. 22, § 1711-E-2.

266. *Mills*, 616 F.3d at 40–41 (Lipez, J., concurring) (noting that pharmacies and data miners under the Maine law must impose a contractual obligation on their customers not to use prescription information for marketing purposes).

267. *Id.* at 41.

B. Ethics-Based Patient Privacy Protections

There are three sets of professional ethical codes or guidelines that represent another possible source for protecting the privacy of patient prescription PHI. However, all of these ethical codes fail to adequately emphasize patient prescription information privacy and raise certain enforcement and compliance weaknesses in terms of their effectiveness.

The first ethical code is the American Medical Association's (AMA) Prescription Data Restriction Program (PDRP), which seeks to curb the use of prescription information in marketing.[268] The PDRP allows prescribers to opt in to a program whereby data miners sell prescription information to pharmaceutical companies, but those pharmaceutical companies are prohibited from giving the data to marketers for a period of three years, with an option for an extension by the prescriber.[269] From the patient privacy perspective, the PDRP fails to provide adequate protection to patient privacy because, like some of the New England data-mining statutes, it allows physicians, but not patients, to restrict detailers' access to prescription information.[270]

Following the AMA's promulgation of the PDRP, PhRMA revised its professional code, the PhRMA Code, to track the provisions of the PDRP.[271] The PhRMA Code announced a commitment by PhRMA to address its own marketing practices to prescribers to curb marketing practices that patients might perceive as inappropriate.[272] Despite this commitment, the PhRMA Code only addresses ethical uses of prescriber data, not patient data. In fact, it condones any "responsible" use of patient data, provided such data de-identifies patients.[273] Moreover, as with the PDRP, the PhRMA Code weakly relies on discretionary and voluntary

---

268. *Mills*, 616 F.3d at 23 n.17 (majority opinion); IMS Health Inc. v. Ayotte, 550 F.3d 42, 74 (1st Cir. 2008); *AMA Program Helps Protect Prescribing Information: Q&A with American Medical Association Trustee Jeremy A. Lazarus*, AM. ACAD. OF NEUROLOGY (Oct. 22, 2008), http://www.aan.com/news/?event=read&article_id=6677.

269. Baxter, *supra* note 47, at 653 (outlining the PDRP program).

270. Orentlicher, *supra* note 5, at 78 (arguing providers should not have sole authority for protecting the privacy interests of patients).

271. Howard L. Dorfman, *The 2009 Revision to the PhRMA Code on Interactions with Healthcare Professionals: Challenges and Opportunities for the Pharmaceutical Industry in the Age of Compliance*, 31 CAMPBELL L. REV. 361, 371 (2009).

272. PHARM. RESEARCH & MFRS. OF AM., CODE ON INTERACTIONS WITH HEALTHCARE PROFESSIONALS 2 (2008), *available at* http://www.phrma.org/sites/default/files/108/phrma_marketing_code_2008.pdf.

273. *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).

compliance for enforcement.[274] Even more troubling is the fact that PhRMA's Code is "promulgated by lobbyist groups within the industry, leaving the neutrality of these guidelines highly questionable."[275]

In the context of patient prescription information privacy, the only ethical code that specifically focuses on patient privacy is the American Pharmacists Association's (APhA) Code of Ethics for Pharmacists. The APhA's Code of Ethics requires pharmacists to place "concern for the well-being of the patient at the center of professional practice" and to serve their patients "in a private and confidential manner."[276] This provision is not as strong as it may seem.

First, not all states impose the confidentiality requirement on pharmacists through the force of law as they do with regard to patient confidentiality and physicians.[277] Second, the APhA Code does not protect the confidentiality of medical information that has been disclosed by a pharmacist to a third party, like a pharmaceutical manufacturer.[278] For example, once information flows from a pharmacy to a data miner or pharmaceutical manufacturer, there is no duty of confidentiality that flows from the drug manufacturer to the patient.[279] Third, even if the pharmacist owes a duty of confidentiality with regard to patient prescription PHI, the individual pharmacist, at least within the context of chain pharmacies, does not control the flow of prescription information. The patient prescription PHI is sent from the patient's individual pharmacy to that pharmacy's out-of-state headquarters where it is aggregated and transferred or sold to data miners or other entities.[280] In other words, the pharmacy corporation determines the transfer of patient prescription information outside of the pharmacy, not the patient's pharmacist. Ethically based pharmacy–patient

---

274. Weiss, *supra* note 55, at 274 (arguing that the PhRMA Code's voluntary compliance provision invites noncompliance). Notably, the PhRMA Code only applies to pharmaceutical companies, whereas the data-collection industry is completely unregulated. Mowery, *supra* note 2, at 701.

275. Connors, *supra* note 7, at 278.

276. *Code of Ethics for Pharmacists*, AM. PHARMACISTS ASSOC., http://www.pharmacist.com/AM/Template.cfm?Section=Search1&template=/CM/HTMLDisplay.cfm&ContentID=2903 (last visited Feb. 19, 2012).

277. Mowery, *supra* note 2, at 717–18 (noting that the APhA's code of ethics is not imposed on pharmacists by common law or statute in all states); Schawbel, *supra* note 3, at 958 (noting that "not all states impose the APhA's code upon pharmacists by law as they do upon doctors with the AMA's Principles of Medical Ethics").

278. Mowery, *supra* note 2, at 718; Schawbel, *supra* note 3, at 958.

279. Schawbel, *supra* note 3, at 960–61 (noting that state laws do not obligate data miners and pharmaceutical companies to maintain a patient's confidentiality in his or her prescription records).

280. IMS Health Inc. v. Ayotte, 550 F.3d 42, 103 (1st Cir. 2008) (Lipez, J., concurring and dissenting) (recounting that data miners' transactions regarding prescription data take place out of state).

confidentiality, in the chain-drug-store context, is only as strong as the pharmacy employer's respect for that confidentiality.[281]

In summary, the ethical codes that govern the privacy of patient prescription PHI, like the New England data-mining statutes, are more focused on protecting the prescriber's information than the patient's prescription PHI. Moreover, even the APhA's Code, which directly focuses on patient privacy, lacks strong enforcement mechanisms to ensure that patient privacy is truly protected.

C. State-Based Remedies to Patient Prescription Privacy Violations Beyond the New England Data-Mining Statutes

While there are a wide range of state constitutional, statutory, and common law remedies available for protecting patient privacy, a state-based approach toward protecting the privacy of de-identified patient prescription PHI is not the best approach. First, state statutes vary in terms of whether they recognize a privacy interest in patient prescription PHI, the level of privacy protection afforded, and how they enforce or regulate such privacy.[282] Accordingly, relying upon state-based statutory protections results in patients in different states having potentially different levels of privacy protection in their prescription records. Thus, entities subject to such regulation would bear the cost and burden of complying with fifty potentially different statutes; further, entities that transmit prescription PHI interstate would have to figure out which states' rules apply and when.[283] This is hardly a model for efficiency, consistency, or cost savings, the latter being of much importance in today's health-care-reform-minded environment.[284]

Second, the right to privacy embodied within state common law and the Restatement is non-comprehensive and provides only modest privacy protection.[285] State privacy tort actions apply in a narrow range of highly

---

281. Schawbel, *supra* note 3, at 956 (arguing that the protection of pharmacist–patient confidentiality is weak, if the pharmacist's employer does not respect it).

282. Han, *supra* note 2, at 135 (arguing for the need for more comprehensive federal regulation to protect the privacy of patient PHI); Schawbel, *supra* note 3, at 925 (arguing that privacy protection of medical records is hindered by the lack of uniformity among state laws); Terry & Francis, *supra* note 78, at 712 (citing Tennessee as an example of a state that rejects the use of the breach-of-confidence tort for purposes of protecting the privacy of health information).

283. Schawbel, *supra* note 3, at 925 (contending that the interstate transfer of health information data exacerbates the weakness inherent in having varying state laws to protect such privacy).

284. Diane T. Carter, *Health Law*, 74 TEX. B.J. 32, 33 (2011) (noting that the Affordable Care Act imposes numerous cost-savings measures to finance health care reform).

285. Terry, *supra* note 6, at 4 (contending that the common law right to privacy "promises far more than it delivers").

qualified circumstances that require patients to "rely on factually restricted, doctrinally limited, and somewhat clumsy protections against 'unreasonable intrusion upon the seclusion of another' or 'public disclosure of private facts.'"[286] Generally, privacy torts have seldom been applied to the field of health care, and when they have been applied, they have only been successful in "a few extreme or outlying cases of medical intrusions or publications."[287]

In the context of a patient–pharmacist relationship, the privacy torts further fail to provide adequate protection because they usually require patients to demonstrate a special relationship between the patient and the pharmacist disclosing the patient's private information.[288] However, pharmacy patients cannot demonstrate such a relationship or expectation of privacy therein because, in contrast to the patient–physician relationship, states do not recognize a special relationship between a patient and pharmacist.[289]

Privacy torts also do not translate well to situations involving third-party use of health information because courts are unlikely to find third-party misuse of such information to be highly offensive to a reasonable person.[290] Nor are state courts likely to find aggregated digital information collected by third parties to be truly private.[291] Significantly, these third-party secondary users are not subject to state-law-mandated obligations of confidentiality.[292]

Third, like the common law, most state statutes are also non-comprehensive in protecting confidential medical information against disclosure; many provide safe harbors and special circumstances under which disclosure is permitted.[293] Many state statutes address narrow, specific informational privacy issues and are "riddled with exceptions."[294]

---

286. Terry & Francis, *supra* note 78, at 711–12 (arguing that common law privacy torts provide inadequate protection for the privacy of health data).

287. *Id.* at 712; *see also* Terry, *supra* note 6, at 4–5 (citing *Knight v. Penobscot Bay Medical Center*, 420 A.2d 915 (Me. 1980), *Estate of Berthiaume v. Pratt*, 365 A.2d 792 (Me. 1976), and *Swarthout v. Mutual Service Life Insurance*, 632 N.W.2d 741 (Minn. Ct. App. 2001) as illustrative of the difficulties in applying common law privacy torts to the field of health care).

288. Mowery, *supra* note 2, at 714.

289. *Id.* at 713 (noting that "[n]o state expressly provides for a pharmacist-patient privilege").

290. DeVries, *supra* note 30, at 288 n.39 (arguing that common law torts provide inadequate protection for informational privacy).

291. *Id.* at 307.

292. Mowery, *supra* note 2, at 716–17 (arguing that since there is no confidential relationship between a pharmaceutical company and a patient, it would be difficult for a patient to sustain a privacy claim against a pharmaceutical company).

293. Terry & Francis, *supra* note 78, at 713 (discussing the weaknesses of state privacy and confidentiality statutes with regard to protecting the privacy of health information).

294. DeVries, *supra* note 30, at 289 (quoting Flavio K. Komuves, *We've Got Your Number: An*

Most state statutes also fail to provide patients with a cause of action for improper disclosure of health information, or do so only when the information is in the hands of the government and not private actors.[295]

Fourth, state constitutional privacy protections have rarely been invoked to protect informational privacy, such as the privacy of patient prescription PHI.[296] Accordingly, state constitutional provisions, the common law, and state statutes each have their shortcomings in terms of protecting the privacy of patient prescription PHI. Generally, the overriding weaknesses inherent in all three sources are a lack of consistency and a limited scope of effectiveness.

D. The Constitutional Right to Privacy, HIPAA, and Patient Prescription-Information Privacy

In terms of federal protections for patient prescription-information privacy, two options outlined above seem most applicable: the constitutional right to privacy and HIPAA. However, upon closer examination, neither adequately or comprehensively protects the privacy of patient prescription PHI, especially de-identified patient prescription PHI.

As to the constitutional right to privacy, a patient generally cannot invoke his or her right to privacy against a data miner, pharmaceutical manufacturer, pharmacy, or any other non-governmental entity.[297] A constitutional right-to-privacy claim requires the plaintiff to allege that a state actor violated the plaintiff's right to privacy.[298] Under the state action doctrine, the Supreme Court has held that the deprivation of a constitutional right—in this case the right to privacy—must be "fairly attributable to the State."[299] The deprivation must be by a state official, be done in concert

---

Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 535 (1998)) (arguing that state and federal statutes designed to protect informational privacy are insufficient to achieve that goal).

295. Terry, *supra* note 6, at 6; Terry & Francis, *supra* note 78, at 713; *see, e.g.*, CAL. CIV. CODE § 56.35 (West 2011); 2001 Haw. Sess. Laws 244; WASH. REV. CODE ANN. § 70.02.170 (West 2011); WIS. STAT. ANN. § 146.84(1)(c) (West 2011).

296. DeVries, *supra* note 30, at 288–89 (criticizing state constitutional privacy protections as inadequately protecting informational privacy).

297. Glenn, *supra* note 90, at 1612 (noting that "constitutional protections lack the capacity to protect privacy invasions from private actors"); Schawbel, *supra* note 3, at 952 (noting that legislation protecting the privacy of prescription records within the private sector is lacking).

298. Edmonson v. Leesville Concrete Co., 500 U.S. 614, 619 (1991) (holding that "[t]he Constitution's protections of individual liberty and equal protection apply in general only to action by the government").

299. Lugar v. Edmondson Oil Co., 457 U.S. 922, 937 (1982).

with or with significant aid from a state official, or must be "otherwise chargeable to the State."[300]

While the transfer of patient prescription PHI to law enforcement agencies or governmental entities for public health purposes might meet the state action test to the extent such transfers are required by law, the holding in *Whalen* probably forecloses any such claim.[301] Even if such claims are viable in the law enforcement and public health contexts, the same cannot be said with regard to transfers of patient prescription PHI to data miners, pharmacies, researchers, and pharmaceutical companies. These latter transfers of identified or de-identified patient prescription PHI are not tantamount to state action. For example, if a patient-plaintiff wanted to join in the CVS Caremark lawsuits, he or she would be precluded from asserting a constitutional privacy claim against CVS Caremark for the alleged privacy violations because CVS Caremark appears to be acting as a private entity.[302] The state action doctrine is particularly troublesome in the context of medical information given that most medical and prescription information in the United States is held by private entities, like CVS Caremark.[303] Therefore, constitutional privacy claims with regard to such information are unlikely to meet the state action test.

The constitutional protection afforded to health information is also too narrow to adequately protect the privacy of patient prescription PHI.[304] To trigger the application of constitutional privacy protection, the health information must be both subjectively and objectively private, rather stringent standards.[305] Even if identifiable patient prescription PHI is deemed to be both subjectively and objectively private—still an open question—de-identified patient prescription PHI is less likely to be so because it is stripped of identifiable characteristics. It may be quite a strain for federal judges to hold that de-identified patient prescription PHI, in its

---

300. *Id.*

301. Whalen v. Roe, 429 U.S. 589, 605 (1977) (noting that the right to privacy in personal information is not absolute in the context of "[t]he collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws"); DeVries, *supra* note 30, at 288 (contending that federal courts are overly deferential to governmental justifications for collecting private personal information).

302. Complaint at 1, Burton's Pharmacy, Inc. v. CVS Caremark Corp., No. 1:11-cv-2 (M.D.N.C. Jan. 3, 2011); Complaint at 5–6, Muecke Co. v. CVS Caremark Corp., No. 6:10-cv-78 (S.D. Tex. Sept. 30, 2010).

303. Schawbel, *supra* note 3, at 942 (discussing why the constitutional right to privacy does not adequately protect the right to privacy in health information).

304. DeVries, *supra* note 30, at 288 (arguing that the constitutionally protected privacy interest in "'avoiding disclosure of personal matters' does not seem very broad" (quoting *Whalen*, 429 U.S. at 599)).

305. *Id.*

de-identified form, is objectively private information. However, this does not mean that there are not important reasons to protect such information.

Like the constitutional right to privacy, HIPAA also fails to fully protect privacy in patient prescription PHI, largely as a result of its narrow scope, loopholes, and enforcement weaknesses. To start with, the HIPAA regulations are dense, complex, confusing, and lengthy.[306] HIPAA's restrictions also suffer from a myopic focus, applying only to health plans, health care clearinghouses, providers who transmit PHI in electronic form, and, in the future, business associates of those actors.[307] For example, pharmaceutical manufacturers are not usually covered entities under HIPAA.[308]

Moreover, the loopholes or exceptions to HIPAA's standards are unduly broad and not controlled tightly enough, particularly in connection with payment for health care services.[309] There are too many ways in which patient prescription PHI can be used and disclosed without patient consent and without violating HIPAA.[310] This is particularly true with regard to the use of patient prescription PHI for purposes related to payment, treatment, and health care operations.[311] The CVS Caremark lawsuits are based upon allegations that demonstrate how entities can share, disclose, and disseminate patient prescription PHI without patient consent and yet still avoid potential HIPAA violations.[312]

---

306. Terry, *supra* note 6, at 31 (criticizing the HIPAA standards as lacking transparency and clarity); Terry & Francis, *supra* note 78, at 715 (arguing that the partial preemption by HIPAA of state privacy protections creates confusion and renders HIPAA operationally obstructive).

307. 45 C.F.R. § 160.102(a) (2010); Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Act, 75 Fed. Reg. 40,868, 40,869 (July 14, 2010) (to be codified at 45 C.F.R. pts. 160, 164) (addressing the expansion of HIPAA restrictions to business associates of covered entities); Terry & Francis, *supra* note 78, at 716 (criticizing HIPAA for its failure to apply privacy protections to all medical data and all users of such data).

308. Hilary M. Wandall, *An Overview of Privacy Laws Impacting Pharmaceutical Companies*, 878 PLI/PAT 509, 516 (2006) (describing the limitations of HIPAA in terms of covered entities, particularly within the pharmaceutical industry).

309. Terry, *supra* note 6, at 31; Terry & Francis, *supra* note 78, at 683–84 (describing HIPAA's privacy protections as "sieve-like").

310. Terry & Francis, *supra* note 78, at 717 (arguing that HIPAA's regulations read like a catalogue of exceptions to confidentiality or a set of "process rules for authorizations to avoid confidentiality").

311. 45 C.F.R. § 164.506(b)(1); Citizens for Health v. Leavitt, 428 F.3d 167, 174, 187 (3d Cir. 2005) (upholding regulatory removal of any requirement of patient consent to disclosure of protected health information for payment, treatment, and health care operations purposes).

312. Complaint at 11, Burton's Pharmacy, Inc. v. CVS Caremark Corp., No. 1:11-cv-2 (M.D.N.C. Jan. 3, 2011) (describing CVS Caremark's alleged justification for sharing patient prescription PHI with the Caremark side of CVS Caremark).

Even outside of treatment and billing, there are many HIPAA-permitted unrestricted uses of patient prescription PHI that do not require patient consent, particularly by secondary users.[313] HIPAA fails to create patient rights and fails to limit the collection and dissemination of PHI but instead focuses on the process of patient consent to disclosure.[314]

Even more significant within the context of this Article, the Privacy Rule expressly excludes de-identified health information from its privacy protections.[315] Accordingly, to the extent that a patient wants to protect his or her de-identified prescription information from being transferred to and used by a data miner or pharmaceutical manufacturer or any other covered entity under HIPAA, the Privacy Rule provides no assistance. HIPAA does not even require the de-identification of patient prescription PHI.[316]

HIPAA's de-identification standards also invite criticism. Even though HIPAA may deem a document containing health information to be de-identified, this is not tantamount to the document being rendered absolutely incapable of re-identification.[317] HIPAA considers data to be de-identified if certain patient-identifying information is removed, such as name, address, and Social Security Number.[318] However, HIPAA does not require other information, such as height, weight, ethnicity, birth year, or the patient's physician to be de-identified with regard to prescription information, and there is no surefire guarantee that such information cannot actually be used to identify the patient.[319]

Not only does HIPAA fail to adequately protect the privacy of de-identified patient prescription PHI, but it also fails to adequately protect the privacy of encrypted patient prescription PHI. The Security Rule defines the term encryption as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use

---

313. Terry & Francis, *supra* note 78, at 715–16; Wandall, *supra* note 308, at 517 (noting that the HIPAA Privacy Rule "permits disclosure of product safety data to pharmaceutical manufacturers . . . without an authorization").

314. Terry & Francis, *supra* note 78, at 714–16 (outlining the flaws and limitations of HIPAA).

315. 45 C.F.R. §§ 164.502(d)(2), 164.514(a)–(b).

316. Terry, *supra* note 6, at 3 (arguing that the U.S. legal system is "only dimly cognizant of the deidentification model").

317. Gellman, *supra* note 16, at 37–38 (noting that HIPAA's Privacy Rule assumes that data de-identified according to the Privacy Rule standards provides complete anonymity, even though it actually carries a risk of re-identification, particularly when public records are consulted for re-identification purposes).

318. 45 C.F.R. § 14.50(d)(1) (requiring removal of eighteen specific identifiers for data to be considered de-identified under HIPAA).

319. Klocke, *supra* note 6, at 511–12 (illustrating what HIPAA de-identified health records might look like).

of a confidential process or key."[320] The Security Rule also requires covered entities, and in the future, business associates, to safeguard electronic protected health information through encryption or a comparable method.[321] Once protected health information is encrypted, HHS considers such information to be adequately protected from disclosure because it considers encrypted protected health information to be rendered "unusable, unreadable, or indecipherable to unauthorized individuals."[322] In fact, in its Interim Final Rule regarding notification of breaches of protected health information, HHS explained that a covered entity need not even provide breach notification to the patient if it encrypts protected health information and later discovers a breach of that encrypted information.[323]

In other words, the breach-notification requirements only apply to breaches of unsecured protected health information.[324] HHS does not appear concerned with using HIPAA to force covered entities to notify patients of breaches of their privacy involving encrypted protected health information. Nor has HHS demonstrated any interest in notifying patients of the uses of their encrypted PHI in its encrypted form. Under existing HIPAA regulatory guidance, it seems that neither patients nor HHS, on behalf of patients, can use HIPAA to protect the privacy of encrypted patient prescription information.

HIPAA also lacks strength in terms of enforcement because it does not provide for a civil action on behalf of patients who are victims of improper disclosure of patient prescription PHI.[325] If a patient-plaintiff joined one of the CVS Caremark lawsuits, he or she would have no litigation recourse through HIPAA. Instead, HIPAA relies on a compliance and regulatory oversight model for enforcement of HIPAA privacy provisions with the possibility for civil or criminal penalties.[326] This enforcement scheme sends

---

320. 45 C.F.R. § 164.304.

321. *Id.* §§ 164.312(a)(2)(iv), (e)(2)(ii); Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40,916–17 (July 14, 2010) (to be codified at 45 C.F.R. pts. 160, 164) (proposing to directly subject business associates to the Security Rule standards).

322. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, 74 Fed. Reg. 19,006, 19,006–08 (Apr. 27, 2009) (to be codified at 45 C.F.R. pts. 160, 164).

323. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740, 42,741–42 (proposed Aug. 24, 2009) (to be codified at 45 C.F.R. pts. 160, 164).

324. Terry, *supra* note 69, at 257.

325. *Id.* at 251 (noting that HHS's Office of Civil Rights has control over HIPAA enforcement rather than patients); Terry & Francis, *supra* note 78, at 713.

326. Terry, *supra* note 6, at 7–8, 13 (describing HIPAA's enforcement mechanism); *see* 45 C.F.R. § 164.530.

the wrong message, that patient prescription-data privacy rights "belong to the healthcare system and not to patients."[327]

Related to enforcement is the question of HIPAA's effectiveness. One study identified 291 publicly reported health-information data breaches from 2003 through 2007, which potentially exposed the health information of more than sixteen million patients.[328] With medical information privacy breaches over a four-year period potentially impacting sixteen million or more patients, one has to ask whether HIPAA goes far enough in protecting patient information privacy. Doubts exist "as to the level of the federal government's commitment to the enforcement of the HIPAA rules."[329]

In summary, neither the constitutional right to privacy nor HIPAA is comprehensive enough to provide sufficient protection for privacy in patient prescription PHI, particularly de-identified patient prescription PHI. Accordingly, there is a demonstrated need for federal legislation to provide comprehensive protection for identifiable and de-identified patient prescription PHI.

V. FEDERAL LEGISLATION TO PROTECT PRIVACY WITHIN PATIENT PRESCRIPTION-HEALTH INFORMATION

A. Elements of a Federal Statute to Protect Privacy Within Patient Prescription-Health Information

Reviewing the available options, existing state and federal privacy protections fail to adequately protect patient privacy in prescription PHI. First, none of the options sufficiently focus on protecting the privacy of de-identified or encrypted prescription PHI. Second, the New England statutes and other state-based options raise Commerce Clause concerns, and more generally, practical concerns regarding a lack of national uniformity in protecting patient prescription information privacy. Third, the New England statutes and the ethical options are more prescriber-centric than patient-centric in their focus. Fourth, in the case of the New England statutes, the ethical options, and HIPAA, patients lack the power to control the privacy and disclosure of their prescription PHI. Finally, compliance weaknesses exist across most, if not all, of the available options.

Any future statutory attempt to protect the privacy of prescription PHI, be it federal or state, must address these weak points. Of particular importance is the lack of protection that patients currently have in guarding

---

327. Terry, *supra* note 6, at 13.
328. Terry, supra note 69, at 236 (citing evidence that medical data is still at risk under HIPAA).
329. *Id.* at 239.

the privacy of their de-identified or encrypted prescription PHI. Patients have a legitimate interest in protecting the privacy of this information because it still provides intimate details about a patient's life and health. Moreover, de-identified information can too easily be re-identified and encrypted information can too easily be decrypted.[330] Patients should legitimately fear that what facially appears to be anonymous may not carry such anonymity in perpetuity. Accordingly, any future statutory attempt to fully protect the privacy of patient prescription PHI must specifically provide for privacy protection of de-identified and encrypted patient prescription PHI.

For practical reasons, any future efforts to provide privacy protection should also be made at the federal level. Unlike state statutes, a federal statute provides a valuable level of uniformity in privacy protection.[331] For example, in the two CVS Caremark lawsuits,[332] two different courts applying two different sets of state laws might come out on opposite sides as to whether CVS Caremark's alleged prescription-information-sharing scheme raises privacy concerns. If different state laws governed, then the end result would be confusion, uncertainty, and inconsistency regarding the lawfulness of the alleged information-sharing scheme.

With a federal statute, every patient, regardless of where he or she lives, has the same level of privacy protection for his or her prescription PHI.[333] Without a federal statute, a patient living in one state could have his or her prescription PHI fully protected in one state, and then suddenly lose that privacy protection simply by moving to a different state.[334] Similarly, a person could live near a state border and fill prescriptions at different pharmacies in each state, receiving differing levels of privacy protection depending on where each prescription was filled.[335] Under these scenarios,

---

330. Gellman, *supra* note 16, at 34–35 (arguing that "[n]o matter how many identifiers have been removed or encrypted and no matter how much data has been coded or masked, the remaining data may still be reidentified").

331. Elizabeth Hutton & Devin Barry, *Privacy Year in Review: Developments in HIPAA*, 1 I/S: J.L. & POL'Y INFO. SOC'Y, JLP 347, 379 (2005) (arguing that additional federal legislation is needed to uniformly protect patient privacy because HIPAA fails to preempt state law); Mowery, *supra* note 2, at 738 (contending that "the likelihood of every state enacting model or uniform laws is very small").

332. Complaint at 21–22, Burton's Pharmacy, Inc. v. CVS Caremark Corp., No. 1:11-cv-2 (M.D.N.C. Jan. 3, 2011); Complaint at 34–37, Muecke Co. v. CVS Caremark Corp., No. 1:11-cv-2 (S.D. Tex. Sept. 30, 2012); Mowery, *supra* note 2, at 735 (arguing that "federal legislation would be able to standardize the management of patient information").

333. Hutton & Barry, *supra* note 331, at 379.

334. Mowery, *supra* note 2, at 718–19 (noting that varying state privacy laws create problems for patients who move from one state to another).

335. *Id.* (noting that varying state privacy laws create problems for patients who receive treatment in different states).

the privacy of an individual's prescription PHI is only as strong as the privacy guaranteed by the state with the weakest privacy provision.

For those required to comply with a prescription PHI privacy statute, a federal statute is beneficial because the regulated entity or individual need not comply with fifty potentially different state privacy statutes.[336] A federal privacy statute would be much less onerous and burdensome on those required to comply with it. For example, in the context of the two CVS Caremark lawsuits, a federal statute would provide national and uniform clarity for CVS Caremark regarding lawful-versus-unlawful uses of patient prescription PHI.

For both patients and those who would use patient prescription PHI, a federal statute would also "more accurately reflect[] the way in which the modern health care system operates."[337] Today, computerized and internet-based information can be accessed across state lines from remote locations; thus, it would be confusing and difficult to determine which state's laws apply with regard to internet-based access to a given set of patient prescription PHI.[338]

Unlike a federal statute, a state statute would also raise enforcement concerns because of states' jurisdictional limits and states' weak enforcement abilities.[339] For example, it is very difficult to enforce in-state violations committed by out-of-state violators, as illustrated by the New England data-mining cases.[340] Moreover, state statutes regulating the electronic transfer and use of information raise thorny questions as to what extent a state can constitutionally regulate extraterritorial conduct.[341]

With a federal statute being the more appealing option, the scope of federal preemption must also be addressed. A federal statute that preempts only less protective laws, similar to the HIPAA statute, would be more protective of privacy, but such an approach carries a significant downside. It would still leave open the possibility that prescription-data users may be subject to different standards and burdens in states that enact more strict

---

336. Klocke, *supra* note 6, at 535 (arguing that "[s]tate-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").

337. Mowery, *supra* note 2, at 739.

338. *Id.*

339. DeVries, *supra* note 30, at 291.

340. *Id.*

341. IMS Health Inc. v. Mills, 616 F.3d 7, 14, 26, 28, 32 (1st Cir. 2010); IMS Health Inc. v. Ayotte, 550 F.3d 42, 63–64 (1st Cir. 2008) (citing K-S Pharms., Inc. v. Am. Home Prods. Corp., 962 F.2d 728, 730 (7th Cir. 1992); State v. McGlone, 78 A.2d 528, 530 (N.H. 1951)).

prescription privacy statutes than the federal law.[342] Accordingly, in terms of simplicity, efficiency, and potential cost savings, a federal law that completely preempts state law is the preferable approach.

In addition to being a completely preemptive federal statute and specifically encompassing de-identified or encrypted patient prescription PHI, any future statute should be more patient-centric, unlike the New England data-mining statutes and the ethics-based options. The latter two options demonstrate a greater concern for how data miners and pharmaceutical companies use prescriber prescription information than any real concern for how such entities and others use patient prescription PHI.[343] The protections encompassed within both alternatives seek to empower prescribers to prevent the disclosure, dissemination, and use of their own information, and do not necessarily empower the patient to do the same with regard to his or her prescription PHI. Therefore, future legislative efforts to protect patient prescription PHI must do just that: focus on protecting the patient's information and not the prescriber's information. It is important that the statute recite, as its purpose, the protection of patient prescription PHI and expressly provide for a method to protect such information.

This leads to the issue of how a future federal statute can best comprehensively protect the privacy of patient prescription PHI, including de-identified and encrypted information. None of the existing options provide a proactive approach for patients to protect the privacy of their prescription information, and certainly not their de-identified or encrypted prescription information. HIPAA only applies to identifiable protected health information[344] and is focused more on notice to the patient regarding use of such information than patient consent for such use.[345] The federal constitutional options and state-based options only provide reactive privacy protection, meaning these options do not empower patients to prevent unauthorized access to their prescription PHI but only allow them to file suit once a breach of privacy occurs. If the CVS Caremark lawsuits involved a patient-plaintiff, the two cases would illustrate how available remedies are reactive. Even though the *Muecke Co.* complaint seeks

---

342. Schawbel, *supra* note 3, at 951–52 (discussing the advantages and disadvantages of complete federal preemption of medical-record-privacy protection).

343. IMS Health Inc. v. Sorrell, 630 F.3d 263, 270 (2d Cir. 2010); *Mills*, 616 F.3d at 12; *Ayotte*, 550 F.3d at 61; Glenn, *supra* note 90, at 1612 (arguing that ethical models for protecting patient privacy are inadequate because they leave too much discretion in the hands of health care providers).

344. 45 C.F.R. §§ 164.502(d)(2), .514(a)–(b) (2011).

345. Terry & Francis, *supra* note 78, at 714–15 (arguing that HIPAA's principal achievement was that it required covered entities to give patients notice of privacy practices, and that HIPAA lacks a consent-to-disclosure requirement for most health care activities).

injunctive relief, the primary focus of the two CVS Caremark lawsuits is really on privacy breaches of patient prescription PHI that have already occurred.[346]

Future legislative efforts to protect the privacy of patient prescription PHI must empower the patient a priori to choose if or how that patient's prescription information will be used.[347] While this may be accomplished in any number of ways,[348] one promising option is to require that the patient be presented with a form upon filling his or her first prescription with a particular pharmacy and each additional pharmacy thereafter. This would allow the patient to opt in to protect the privacy of his or her identifiable, de-identified, and encrypted prescription information.[349] The patient could alter his or her decision at any time by filling out a new form.

This opt-in privacy form would have two boxes: one for opting in to protect the privacy of identifiable prescription information and one for opting in to protect the privacy of de-identified and encrypted prescription information. The patient could choose to check one box, both boxes, or neither box. If neither box is checked, then the patient is effectively permitting use of his or her identifiable, de-identified, and encrypted prescription information for any use otherwise permitted under law. Admittedly, this process does require a heavy educational component for patients, which may be time-consuming for providers to perform and difficult for patients to understand.

A few points require elaboration or clarification. First, even though the use of identifiable prescription information is already restricted under many situations,[350] the check box for protection of identifiable prescription information is still necessary. As outlined above, the existing options for protecting patient prescription PHI are non-comprehensive. As an example of existing loopholes, the CVS Caremark lawsuits involve situations in which CVS Caremark is allegedly using a creative corporate structure to

---

346. *See generally* Complaint, Burton's Pharmacy, Inc. v. CVS Caremark Corp., No. 1:11-cv-2 (M.D.N.C. Jan. 3, 2011); Complaint, Muecke Co. v. CVS Caremark Corp., No. 6:10-cv-78 (S.D. Tex. Sept. 30, 2010).

347. Rosoff, *supra* note 2, at 26 (contending that people want to be able to control who has access to their medical information); Terry & Francis, *supra* note 78, at 719 (citing a survey demonstrating that 79% of respondents viewed it as a top priority that their electronic health information only be shared with others with the patient's consent).

348. Terry & Francis, *supra* note 78, at 701–03 (describing various options for protecting patient privacy in electronic health record systems, including allowing patients to specify that records from certain providers or certain types of information from their medical records be kept out of electronic health record systems).

349. *Id.* at 701 (describing an opt-in system within the context of electronic health records where patients who do not opt-in would have their records siloed).

350. *See generally* 45 C.F.R. pts. 160, 164 (2010).

avoid HIPAA requirements and lawfully share patient prescription PHI.[351] Nonetheless, many patients may still object to the manner in which CVS Caremark is allegedly sharing their identifiable patient prescription PHI, and those patients should retain express control over how their identifiable patient prescription PHI will be used.

Second, two boxes on the opt-in form are necessary because some patients may not be concerned about the use of their de-identified or encrypted prescription information but may still be concerned about the use of their identifiable prescription information. Patients should have flexibility to choose to what extent they wish to exercise their privacy rights.

Third, it may be tempting to want to provide patients with more than two options regarding how they want to allow their prescription information to be used or shared, including, for example, allowing their information to be disclosed for some purposes, but not for others. Ideally, more choice provides more empowerment for patients. However, tracking many different categories of prescription information use for compliance and enforcement purposes would probably be a logistical nightmare. That said, providing more categories for authorizing how one's prescription information may be used might actually be more likely to survive constitutional First Amendment scrutiny. As the Supreme Court held in *Sorrell*, opt-in provisions do not necessarily preclude a statutory burden on free speech from being held unconstitutional if the options provided "are too narrow to advance legitimate interests or too broad to protect speech."[352]

Fourth, it is important that the opt-in form provide a disclaimer that regardless of the choice made by the patient, the patient's prescription PHI may still be used for law enforcement, public health, payment, and treatment purposes. As a practical matter, it would be unreasonable to restrict the use of prescription information for payment and treatment purposes. Insurers and related entities have a legitimate need for patient prescription information in order to engage in important activities, such as ensuring proper payment, identifying payment errors, and avoiding fraud.[353]

---

351. Complaint at 11, Burton's Pharmacy, Inc. v. CVS Caremark Corp., No. 1:11-cv-2 (M.D.N.C. Jan. 3, 2011).

352. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2669 (2011).

353. Whalen v. Roe, 429 U.S. 589, 602 (1977). *Whalen* held:

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

Equally so, health care providers have a legitimate need to gain access to prescription information as part of treating a patient.[354] Finally, as established under *Whalen* and *Citizens for Health v. Leavitt*, federal case law weighs against the constitutionality of prohibiting the sharing of patient prescription PHI for law enforcement and public health purposes.[355]

Enforcement is another area of weakness within existing alternatives for protecting the privacy of patient prescription PHI. As discussed with regard to the New England statutes, unusual enforcement mechanisms and attempts to indirectly regulate downstream marketing allow data miners and pharmaceutical manufacturers to potentially use patient prescription PHI in an unlawful manner without discovery by the patient or state.[356] Moreover, under HIPAA, enforcement is entirely within the control of HHS, which has demonstrated weak enforcement in the past.[357]

To remedy these enforcement weaknesses, future legislative action to protect the privacy of patient prescription PHI should allow patients to track their identifiable, de-identified, or encrypted prescription information, where it goes, who uses it, and for what purposes.[358] If a person can track a FedEx package as it moves across the world, there is no reason why software cannot be developed to allow a patient to track his or her prescription information, regardless of whether the information is identifiable, de-identified, or encrypted. A patient should be able to use a code assigned to his or her prescription information to track where the information goes.[359] Such patient empowerment should deter violations of prescription privacy.

> having responsibility for the health of the community, does not automatically amount to an impermissible invasion of privacy.

Id.

354. *Id.*

355. Terry & Francis, *supra* note 78, at 704 (describing public health and law enforcement scenarios in which health information cannot be kept confidential).

356. IMS Health Inc. v. Mills, 616 F.3d 7, 40–41 (1st Cir. 2010) (Lipez, J., concurring).

357. Tim Wafa, *How the Lack of Prescriptive Technical Granularity in HIPAA Has Compromised Patient Privacy*, 30 N. ILL. U. L. REV. 531, 551–52 (2010) (describing a "major uproar by privacy advocates [that] has emerged over the lack of enforcement action by regulators over HIPAA"). With the passage of HITECH, penalties are increased and there are mandatory penalties for violations due to willful neglect, which may lead to strengthened enforcement. Janine Hiller, *Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared*, 17 B.U. J. SCI. & TECH. L. 1, 18 (2011).

358. Terry & Francis, *supra* note 78, at 719 (citing a survey that demonstrated that 91% of respondents wanted "mechanisms in place to confirm the identity of anyone using the [electronic medical record] system and to guarantee against unauthorized access"); *id*. at 704–06 (describing the need for and importance of a tracking system within the context of electronic health records and advocating for patient notification of unauthorized disclosures).

359. Betty M. Ng, *Universal Health Identifier: Invasion of Privacy or Medical Advancement?*, 26 RUTGERS COMPUTER & TECH. L.J. 331, 354 (2000) (proposing the use of encrypted keys for

Admittedly, this tracking system is not perfect. There are weaknesses. First, to implement such a system would be expensive and burdensome for the government, pharmacies, data miners, pharmaceutical manufacturers, and others who would use patient prescription PHI. Second, the system may be difficult for low-income patients, vulnerable patients, and non-computer-savvy patients to use. Third, the tracking system needs to be secure against hacking.[360] Fourth, by attaching a code to de-identified or encrypted patient information for tracking purposes, one actually creates a risk of re-identification.[361] The patient's code raises a risk that the patient could be identified in relation to a particular set of prescription information if someone breaks the code. Fifth, the system has to be developed in such a way that patients and government regulators can detect any breach of privacy.

The risks of re-identification and decryption might not be as great as they first appear; the code is only circulated among those entities that would have legitimate access to the patient's identifiable prescription information, such as an insurer or treating health care provider. Moreover, in order to empower patients and enhance their ability to restrict and monitor the flow of their prescription PHI, there has to be some trade-off in terms of bearing a risk of re-identification or decryption. Still, for effective enforcement, the tracking system must be capable of detecting when de-identified or encrypted patient prescription PHI is unlawfully rendered identifiable.

Though the tracking system represents great progress towards patient empowerment, the system alone is not sufficient to deter violations. For more effective deterrence, HHS should also conduct audits of the tracking system.[362] HHS should be able to audit the tracking system to determine whether prescription information that was "tagged" by the patient as privacy-protected was unlawfully transferred to entities other than law enforcement, public health entities, and those needing the information for

---

unlocking an individual's universal health identifier, which could only be unlocked by the person in possession of the key); *see* Mowery, *supra* note 2, at 736 (arguing that "security measures can be designed so that personal identifiers restrict entry into the information system, or restrict users to only certain levels of information").

360. Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 938 (2003) (contending that "[i]t is generally accepted that the threat of being hacked has led to a revolution in computer security").

361. Gellman, *supra* note 16, at 34 (arguing that "statistical, encryption, or other mathematical approaches to deidentification aimed at protecting privacy fail to provide solutions to address all data types and data sharing activities").

362. Terry & Francis, *supra* note 78, at 704–06 (proposing tracking or auditing within the context of electronic health records because of the ease with which electronic information can be erased, cut and pasted, stolen, duplicated, altered, and hacked).

payment or treatment purposes.[363] Similarly, HHS audits should focus on identifying when encrypted or de-identified information has been unlawfully rendered identifiable.

When HHS discovers violations, it should also be empowered and encouraged to impose heavy civil monetary penalties on violators. Only strong enforcement with sufficiently heavy penalties will bring about effective deterrence.[364] Even so, to make deterrence even more effective, patients should also be empowered to file a statutory cause of action against violators, along with the potential for damages in a statutorily-set dollar amount per violation. Combined, the HHS and patient-enforced deterrence mechanisms should place an adequate check on entities that may wish to violate the statute in the hopes that they will not get caught.

B. The Proposed Patient-Prescription-Health-Information Statute Under Sorrell

Any analysis of future legislative efforts to protect identifiable, de-identified, and encrypted patient prescription PHI must also address the First Amendment issues raised by the Supreme Court's *Sorrell* decision. Legislation that seeks to protect the privacy of patient prescription PHI will simultaneously limit the use of that information, which, in turn, will likely burden First Amendment commercial speech.

Nonetheless, the envisioned statute would seem more likely to survive First Amendment constitutional scrutiny than the Vermont statute in *Sorrell*. First, with regard to the proposed statute, the substantial governmental interest at stake is the government's interest in protecting a patient's right to privacy in patient prescription PHI, including de-identified and encrypted prescription PHI.[365] Conversely, in *Sorrell*, the focus of the Vermont statute was protecting the prescriber's privacy interest, and the Court never addressed whether or not such an interest is a substantial governmental interest for First Amendment purposes.[366]

Even though the *Sorrell* Court never evaluated the strength of Vermont's asserted interest in protecting prescriber privacy, the strength of the patient's privacy interest should be much stronger than the prescriber's

---

363. Mowery, *supra* note 2, at 736 (discussing the use of audits to determine who has used patient information and for determining whether such access was fraudulent).

364. Weiss, *supra* note 55, at 289 (arguing that the extraordinary profits of the drug industry lead some companies to accept low fines for violations as a cost of doing business).

365. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 564 (1980) (holding that restrictions on commercial speech must be justified by a substantial state interest).

366. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2668 (2011).

privacy interest. Many federal courts have recognized the former to be a constitutionally guaranteed right, albeit a non-absolute right.[367] The same cannot be said as to the existence of a prescriber's constitutional right to privacy, and arguably, any claim by a prescriber to privacy within the physician–patient relationship is actually a privacy-right derivative of the patient's right to medical privacy.[368] Accordingly, the patient's right to privacy should carry more weight under a commercial speech analysis than protecting a prescriber's right to privacy.

This leads to the next issue of whether the statute envisioned in this Article would promote a substantial governmental interest in patient privacy and whether it would be narrowly tailored enough to pass constitutional muster.[369] The former should be self-evident as the proposed statute would plainly protect, by choice of the patient, the privacy of patient prescription PHI, including de-identified and encrypted information, save in a few limited circumstances involving payment, treatment, law enforcement, and public health.

As *Sorrell* demonstrates, the key question is whether the proposed statute is narrowly tailored enough to pass First Amendment scrutiny. In *Sorrell*, the Supreme Court held that the Vermont statute was not narrowly drawn to protect prescriber privacy interests because it allowed prescriber-identifying information to be used in almost limitless situations save one—drug detailing.[370] Moreover, even though Vermont prescribers, and not the state, determined whether or not to invoke their privacy rights through an opt-in mechanism, the Court held that the option to choose privacy—only with regard to detailing—unconstitutionally required prescribers to invoke privacy protection only if they did so "on terms favorable to the speech the State prefers."[371]

Unlike the strict conditions attached to the privacy opt-in approach under the Vermont statute, the proposed statute allows patients to opt in to protecting the privacy of their prescription PHI for all uses except payment, treatment, law enforcement, and public health purposes. In other words, there are only narrow exceptions to patient prescription PHI privacy under

---

367. Whalen v. Roe, 429 U.S. 589, 603–04 (1977); Douglas v. Dobbs, 419 F.3d 1097, 1102 (10th Cir. 2005); Doe v. Se. Penn. Transp. Auth. (SEPTA), 72 F.3d 1133, 1139–40 (3d Cir. 1995).

368. Planned Parenthood of Se. Penn. v. Casey, 505 U.S. 833, 884 (1992) (holding that any constitutional status afforded to the doctor–patient relationship is derivative of a woman's privacy right in the context of abortion rights); Klocke, *supra* note 6, at 518 (arguing that a lapse in physician privacy is "derivative of a lapse in the patient's privacy").

369. *Central Hudson*, 447 U.S. at 364–65 (holding that restrictions on commercial speech must be narrowly tailored to directly promote a substantial state interest).

370. *Sorrell*, 131 S. Ct. at 2668.

371. *Id.* at 2669.

the proposed statute. This would seem to align with the Court's statement in *Sorrell* 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."[372]

Moreover, given the narrow privacy exceptions within the proposed statute, the opt-in mechanism also strengthens the proposed statute's constitutionality. In *Sorrell*, the Supreme Court recognized that private party opt-in mechanisms can result in finding certain burdens on free speech to be constitutional.[373] However, the Court frowned upon Vermont's opt-in mechanism because it made privacy protection available, but under such narrow terms that it required prescribers to essentially favor the State's viewpoint on detailing over any other viewpoint in choosing to invoke their privacy rights.[374]

By contrast, the privacy exceptions in the proposed statute do not favor a particular viewpoint. Rather, they exist out of necessity and practicality. In the case of public health and law enforcement, the exceptions exist because the federal courts have allowed the nascent constitutional right to privacy in health information or prescription information to be overridden by both public health and law enforcement interests. Accordingly, the proposed statute's opt-in mechanism is not used to favor particular content or a particular viewpoint in commercial speech.

As part of the narrow tailoring analysis, it is also notable that unlike the New England statutes, a challenge to the proposed statute would pit two constitutionally guaranteed rights against each other. A data miner or pharmaceutical manufacturer challenging the proposed statute would claim that the statute violates that entity's commercial speech rights, but at the same time, the statute would also exist to protect the patient's constitutional right to privacy in medical information. No existing case law suggests that prescribers have a constitutional right to privacy in their identifiable prescriber information. However, case law does support the assertion that patients have some sort of constitutional right to privacy in their medical information.[375] The result is that the proposed statute embodies a conflict between the patient's constitutional right to privacy in his or her

372. *Id.* at 2672.

373. *Id.* at 2669.

374. *Id.*

375. *Id.* at 2672 ("The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure."); Whalen v. Roe, 429 U.S. 589, 605 (1977); Douglas v. Dobbs, 419 F.3d 1097, 1102 (10th Cir. 2005); Doe v. Se. Penn. Transp. Auth. (SEPTA), 72 F.3d 1133, 1139–40 (3d Cir. 1995); United States v. Sutherland, 143 F. Supp. 2d 609, 611–12 (W.D. Va. 2001).

prescription information and the prescription-information user's right to free speech.

An analogous conflict of constitutional rights has previously arisen within the context of pharmacist-conscience laws, which protect pharmacists from being compelled to dispense contraceptive drugs to patients.[376] Such conscience laws create a conflict between a pharmacist's right to free exercise of religion—that is, not being forced to supply contraceptive drugs against the pharmacist's religious beliefs—and a patient's privacy right to access birth control or abortion medications.[377] Scholars disagree as to which right should prevail within the context of the conscience laws,[378] thus demonstrating the difficulty in determining which constitutional right prevails when two constitutional rights conflict. Not surprisingly, it is difficult to anticipate whether a pharmaceutical company's right to free speech in the context of detailing outweighs the

---

376. *See* Lora Cicconi, *Pharmacist Refusals and Third-Party Interests: A Proposed Judicial Approach to Pharmacist Conscience Clauses*, 54 UCLA L. REV. 709, 713–22 (2007) (outlining the history and evolution of legislation related to pharmacy-refusal clauses); Michael E. Duffy, *Good Medicine: Why Pharmacists Should Be Prescribed a Right of Conscience*, 44 VAL. U. L. REV. 509, 522–27 (2010) (describing and defining the provisions of pharmacy right-to-conscience laws); Jane W. Walker, *The Bush Administration's Midnight Provider Refusal Rule: Upsetting the Emerging Balance in State Pharmacist Refusal Laws*, 46 HOUS. L. REV. 939, 945 (2009) (defining pharmacist "conscience" or "refusal" laws as "laws protecting health care providers who decline to participate in certain health services based on a religious or moral objection").

377. Cicconi, *supra* note 376, at 748 (outlining how refusal laws might be found to burden a woman's right to make a decision to prevent conception, while at the same time protecting a pharmacist's religious-based right not to be compelled to assist the woman in accomplishing that goal); Nancy K. Kubasek, Daniel C. Tagliarina & Corrine Staggs, *The Questionable Constitutionality of Conscientious Objection Clauses for Pharmacists*, 16 J.L. & POL'Y 225, 258 (2007) (arguing that refusal laws place the pharmacist's right to object to providing birth control medication to a patient for religious reasons "in direct conflict with women's constitutional right to privacy").

378. *Compare* Maryam T. Afif, *Prescription Ethics: Can States Protect Pharmacists Who Refuse to Dispense Contraceptive Prescriptions?*, 26 PACE L. REV. 243, 271–72 (2005) (arguing that refusal laws unconstitutionally interfere with a woman's right to access contraceptives and that such laws are too vague in encompassing pharmacist objections, which are moral, as well as religious-based), *and* Taylor Genovese, *Prescribing Morality: The Constitutionality of Pharmacist Conscience Clauses*, 34 HASTINGS CONST. L.Q. 111, 128 (2006) (arguing that most state refusal laws are not narrowly tailored enough to survive constitutional scrutiny with regard to the burden imposed on a woman's right to privacy), *and* Kubasek et al., *supra* note 377, at 261 (arguing that "the constitutional right to privacy and potential obstacles to obtaining birth control outweigh pharmacists' interest in exercising their religion"), *and* Cristina Arana Lumpkin, *Does a Pharmacist Have the Right to Refuse to Fill a Prescription for Birth Control?*, 60 U. MIAMI L. REV. 105, 107 (2005) (arguing that a "pharmacist's right to follow his conscience must yield to a woman's privacy right to make her own reproductive choices"), *with* Duffy, *supra* note 376, at 557 (arguing that ultimately the pharmacist's right to freedom of religion prevails over the patient's right to privacy because the refusal to provide contraceptives to a patient merely results in a delay in access and does not preclude patient access to those drugs), *and* Jason R. Mau, Stormans *and the Pharmacists: Where Have All the Conscientious Rx Gone?*, 114 PENN. ST. L. REV. 293, 330 (2009) (arguing that more federal courts are recognizing the pharmacist's free exercise right within the context of conscience laws).

patient's right to privacy in his or her prescription information or vice versa. Notably, neither right is an absolute right; either may be subject to regulation under certain circumstances.[379]

Despite the difficulty in trying to predict which constitutional right will prevail within the context of the proposed statute, the patient's right to privacy in prescription PHI should prevail over any detailer's commercial speech claim. Generally, courts have allowed patient prescription privacy rights to be curtailed in only limited circumstances where there are very strong governmental interests at stake, such as law enforcement[380] or drug abuse concerns.[381] By contrast, a private third party's interest in access to an individual's private medical information for purposes of creating commercial speech to market drugs and earn a profit hardly rises to a level of importance equal to the government's interest in public health or law enforcement.

Moreover, when privacy rights and commercial speech rights "have come into conflict, privacy has traditionally won."[382] Even when the *Sorrell* Court held that the Vermont statute unconstitutionally burdened commercial speech, it never addressed the issue of whether the prescriber's privacy interest outweighed the detailer's commercial speech interest; the Court merely held that the statute was not narrowly tailored to protect the state's asserted privacy interest.[383]

CONCLUSION

Existing options for protecting the privacy of patient prescription PHI are neither comprehensive nor adequate. The available options are too narrow in their focus, as in the case of the New England data-mining statutes; contain too many loopholes, as in the case of HIPAA; fail to focus on the patient, as in the case of professional ethics codes; or are completely reactive in their approach, as in the case of the federal and state causes of action available for breaches of privacy or confidentiality. Even if the

---

379. Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978) (holding that the Supreme Court has "afforded commercial speech a limited measure of protection, commensurate with its subordinate position in the scale of First Amendment values"); *Whalen,* 429 U.S. at 603–04; *Douglas*, 419 F.3d at 1102 n.3; *SEPTA*, 72 F.3d at 1139–40 (collectively recognizing that there is no absolute right to privacy in prescription information).

380. *Whalen*, 429 U.S. 603–04 (allowing restriction on right to privacy in patient prescription information for purposes of monitoring illegal drug diversion).

381. *SEPTA*, 72 F.3d at 1143 (allowing restriction on right to privacy in patient prescription information for purposes of monitoring a prescription plan for fraud).

382. Klocke, *supra* note 6, at 531.

383. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2668 (2011).

available options offer some positive attributes in terms of protecting the privacy of identifiable patient prescription PHI, they are woefully lacking in protecting the privacy of de-identified or encrypted patient prescription PHI, an overlooked area.

Although the *Sorrell* Court ruled against the most direct attempt to regulate prescription information privacy in the face of commercial speech interests, the *Sorrell* decision does not foreclose all options for protecting a patient's right to privacy in his or her prescription PHI. In fact, the Court hinted at approval for future legislative attempts at protecting prescription information privacy when those efforts provide narrow and well-justified privacy exceptions, do not favor a particular viewpoint, and empower the individual, not the government, to choose when and how privacy protection should be invoked.

The proposed statute herein is tailored to address the Court's concerns and to provide patients with a comprehensive federal statute that will survive constitutional scrutiny and uniformly protect the privacy of patient prescription PHI. The proposed statute attempts to fill in existing gaps in patient privacy protection and strengthen weaknesses in existing options. Specifically, it protects the privacy of de-identified and encrypted patient prescription PHI, as well as identifiable patient prescription PHI. It also completely preempts state law, adopts a patient-centric approach, provides for tracking of privacy breaches, and provides for strong, meaningful enforcement. It is important to empower patients with the confidence that the information that they provide to their pharmacists remains confidential and private, whether such information is identifiable, de-identified, or encrypted. Patients should not have to wonder "who's watching me" when it comes to their patient prescription PHI.