Somebody's Watching Me: Protecting Patient Privacy in De-Identified Prescription Health Information

Christopher R Smith, American University Washington College of Law

Available at: https://works.bepress.com/christopher_smith/6/
SOMEBODY’S WATCHING ME: PROTECTING PATIENT PRIVACY IN DE-IDENTIFIED PRESCRIPTION HEALTH INFORMATION

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.” 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 such information is being used. In today’s ever expanding world of internet technology, 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.

Recent legislative and judicial attention on the use of prescription data has mostly focused 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, as opposed to the privacy concerns of patients with regard to the use of such data. Moreover, while scholarly analysis has focused more on patient privacy within prescription data, there are few articles examining patient privacy within de-identified patient health data, and most of those articles addressing de-identified patient health data do not focus specifically on patient prescription data. Therefore, there is a need for further exploration of the privacy issues surrounding de-identified patient prescription PHI.

In 2009, Americans filled 3,679,671,222 prescriptions. Each of those prescriptions represents a disclosure of personal health information (“PHI”) from the patient to others. Every time a patient fills a prescription, the pharmacy collects, within its computerized database, a host of PHI, including the name of the patient, the patient’s address, the date and place the
prescription is filled, the patient’s age and gender, the identity of the prescribing physician, the drug prescribed, its dosage, and the quantity dispensed.⁹

Most patients probably give little thought to disclosing their PHI to pharmacies because they assume that the disclosed information is used by the pharmacist, and perhaps the doctor, for treatment purposes and/or is used by their insurance companies for purposes of processing the prescription claim and providing coverage for that claim.¹⁰ Patients probably think even less about how their prescription PHI is used once it is de-identified.¹¹ However, most patients are probably not aware of who else sees their prescription PHI or how else that PHI is being used, whether that information is identifiable or de-identified.¹² Regardless of this level of awareness, serious privacy concerns, as outlined infra, surround pharmacy transmissions of both identifiable and de-identified PHI to outside entities for purposes other than insurance reimbursement, treatment, public health and law enforcement. The list is quite long of entities that seek access to patient prescription PHI, 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 de-identified patient prescription PHI. Section I begins by providing context for why there is need for comprehensive federal legislation to protect patient prescription PHI, with a particular focus on why there is a need to protect de-identified patient prescription PHI. Section II then outlines the data mining process for collecting patient prescription PHI and how that data is used. Section III then discusses the backdrop of existing federal and state law protecting patient privacy rights, including patient privacy rights in prescription PHI. Section III particularly focuses on the three recent state statutory attempts to directly curb prescription data mining for marketing purposes and the judicial response to those efforts. Section IV evaluates existing
state, federal and related options available for protecting patient prescription PHI against unauthorized disclosure, with an emphasis on de-identified prescription PHI. This section evaluates the effectiveness of using the data mining state statutes, ethical guidelines, federal constitutional and statutory law and other state law options for protecting the privacy of de-identified patient prescription PHI. Finally, Section V proposes a legislative construct for a federal statute to empower patients with more control over the use of and to protect their privacy in de-identified patient prescription 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, de-identified or encrypted and stripped of identifiable characteristics prior to being transferred to those not authorized to access the identifiable data.\textsuperscript{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 genetic signature, which \textit{ipso facto} prevents the data from ever becoming truly de-identified.\textsuperscript{15} Moreover, even data that appears to be totally de-identified can all too easily be re-identified through various processes, such as geo-coding.\textsuperscript{16} One scholar notes that 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.”\textsuperscript{17}

Additionally, safeguards put into place to protect against attempts at re-identification may not be sufficient.\textsuperscript{18} This vulnerability is particularly problematic when the entity holding the data asserts in its privacy policy their de-identified data “cannot be linked to personal data by third
parties receiving the anonymous information." Furthermore, even if the company collecting the de-identified data maintains a strong privacy policy, there is no guarantee that the buyer of the data will maintain a similarly strong policy.

Unfortunately, there exists no standard identifying the level of identifier-stripping necessary to guarantee that de-identified data cannot be re-identified. In fact, "no 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 re-identified." The ever growing amount of personal information available from public sources makes it all that much easier to re-identify de-identified personal information. Likewise, once an individual’s privacy is breached by re-identification additional and future re-identification also becomes easier to accomplish.

Encrypted PHI, as distinguished from de-identified PHI, carries its own set of concerns. First, encryptions are merely codes and almost all codes can be broken. Moreover, encryption requires use of a key or cipher, which is used to lock and unlock the hidden data. 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. However, there is always a risk that the encryption key may fall into the wrong hands and be accessed by unauthorized viewers.

Patient prescription PHI whether encrypted or de-identified also deserves protection because of the subjective concern of patients for their privacy in their prescription PHI, even if such information is facially de-identified. 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 him or her and knows that someone or some entity out there is viewing that information without the consent of patient “x”.

4
The mere awareness of patient “x” that his or her information is being disseminated without his or her consent may still cause that patient 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 or her consent, but with the face removed and any other identifying features removed.\textsuperscript{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 the content.”\textsuperscript{30}

Even if the risks and concerns surrounding privacy rights in de-identified or encrypted patient prescription PHI alone do not justify the need for comprehensive federal legislation to protect patient prescription PHI, arguably existing protections, such as the Health Insurance Portability and Accountability Act\textsuperscript{31} (“HIPAA”), do not go far enough to protect even identifiable patient 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 CVS Caremark.\textsuperscript{32}

In \textit{The Muecke Company, Inc. v. CVS Caremark Corporation}, pending in the Southern District of Texas, plaintiffs allege that the Caremark or PBM side of CVS Caremark, while coordinating drug benefits between patients, their insurance companies and non-CVS pharmacies, is collecting identifiable prescription health information and transferring that information to CVS pharmacies.\textsuperscript{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.\textsuperscript{34} Caremark then allegedly shares that information through an information technology platform with the CVS or pharmacy side of CVS Caremark.\textsuperscript{35}

Plaintiffs allege that once CVS has the patient PHI, it uses the identifiable PHI in ways that would be troubling to many patients. 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.”\textsuperscript{36} 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.”\textsuperscript{37}

In a North Carolina federal court, a very similar lawsuit was also recently filed against CVS in the case of \textit{Burton’s Pharmacy, Inc. v. CVS Caremark Corporation}.\textsuperscript{38} In \textit{Burton’s Pharmacy, Inc.}, Plaintiffs raise almost identical allegations to those raised in \textit{The Muecke Company, Inc.}\textsuperscript{39} 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.\textsuperscript{40} Plaintiffs further claim that CVS “pitches to drug manufacturers its own ability to use this process to market prescription drugs to patients.”\textsuperscript{41} 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 tailored to specific patient characteristics or demographics, and discount offers to patients to purchase over-the-counter drugs at CVS.\textsuperscript{42}

The Plaintiffs in \textit{The Muecke Company, Inc.} also explain how Caremark allegedly avoids possible HIPAA violations in sharing the non-CVS pharmacy patient data.\textsuperscript{43} Plaintiffs cite to CVS Caremark’s Notice of Privacy Practices, which states that CVS and Caremark view
themselves as part of an affiliated group of pharmacies and that those affiliated pharmacies are treated as a single entity for purposes of sharing information about patients.\textsuperscript{44} In other words, if Caremark has authorized access to a patient’s prescription PHI, it can share that information with CVS pharmacies because they are all considered to be a single entity by CVS Caremark for HIPAA purposes. 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.\textsuperscript{45}

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 CVS’s alleging gaming of HIPAA justify the need for comprehensive federal legislation to protect patient prescription PHI.

II. The Data Mining and Detailing Process

Outside of the situations involved in the pending CVS cases outlined above, 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 raw data, including patient demographic information and patient drug information, which pharmacies, hospitals and insurance companies collect on patients and prescribers.\textsuperscript{46} The raw data that the data miners collect is anonymized, as the data miners install software on pharmacies’ computers to encrypt the patient prescription data before they receive it, so that data miners cannot identify individual patients by name.\textsuperscript{47} Even though patient names are deleted, the data miners replace the patient’s
identifying information with a number, so that they can still track the “de-identified” patient over
time and correlate that particular patient with the various prescriptions filled by that patient.48

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.49 These
reports and databases allow for the examination of multiple transactions involving the same
prescriber to identify that prescribers’ prescribing history, preference of brand-name versus
generic drugs and willingness to prescribe new FDA approved drugs.50 These databases and
reports are very important to brand-name pharmaceutical companies who purchase them from
the data miners.51 The brand-name pharmaceutical companies use the databases and reports to
determine their sales representatives’ marketing strategies directed at the very same prescribers
whose information forms the foundation of the databases and data reports.52 These sales
representatives, also known as detailers, use this data to enhance their detailing or sales visits to
those prescribers.53

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).”54 Drug 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.”55
Second, the databases and reports help detailers to more effectively make their sales pitch to prescribers because knowing a prescriber’s prescribing history allows the detailer to hone in on the unique prescribing behaviors of each individual prescriber.\textsuperscript{56} For example, the detailer who knows that a prescriber is using a competing product can more effectively craft his or her presentation to highlight the weaknesses of the competitor drug.\textsuperscript{57}

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.\textsuperscript{58} However, some argue that pharmaceutical manufacturers’ detailing educational material is very biased with a sole focus on maximizing profit and not safely treating the patient.\textsuperscript{59} Critics contend that the prescribing of prescription drugs “should be dominated by scientific evidence, not secretive marketing techniques.”\textsuperscript{60}

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.\textsuperscript{61} Once a detailer obtains access to a provider, the detailer tries to develop an ongoing relationship with the provider, so that the provider will maintain brand loyalty to the detailer’s manufacturer and will continue to prescribe that manufacturer’s brand-name drug.\textsuperscript{62}

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.\textsuperscript{63} Brand name pharmaceutical companies make annual profits between 15% and 20%, which is far above other industries’ profit margins.\textsuperscript{64} In 2005, one data mining company brought in revenues of $1.75 billion dollars through selling prescriber information databases and reports to brand-name drug companies.\textsuperscript{65}
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.\textsuperscript{66} Accordingly, it is no surprise that detailing represents a massive marketing campaign.\textsuperscript{67} 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.”\textsuperscript{68} 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.\textsuperscript{69} Shockingly, pharmaceutical companies spend more on marketing to prescribers than they spend on research or direct-to-consumer advertising.\textsuperscript{70}

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 results in prescribers overprescribing expensive brand-name drugs, when equally effective generic drugs are available, resulting in greater costs to individual patients, as well as insurers, Medicare Part D plans and Medicaid.\textsuperscript{71} This is significant given that total retail drug spending was over $217 billion for 2009\textsuperscript{72} and given that the growth rate of brand-name drug costs has been two to three times the rate of inflation.\textsuperscript{73}

Second, the detailing and resulting overprescribing of brand-name drugs threatens patient health in cases in which the effects and potential health risks of generic equivalents are more well known than those associated with the brand-name drug.\textsuperscript{74} Detailing causes prescribers to overprescribe unnecessarily risky brand-name drugs to their patients.\textsuperscript{75} Detailing and the free drug samples create a conflict of interest for doctors with regard to their patients.\textsuperscript{76} Moreover, if patient health outcomes suffer as a result, then health care costs also rise, including the patient’s
costs. Arguably, pharmaceutical 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].”

For purposes of this article, the most troubling negative 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 believe that the privacy of their health information is adequately protected. 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. As to the latter, inadequate protection of identifiable and de-identified patient prescription PHI chills patient open communication with their pharmacist, hindering the ability of the pharmacist to provide proper counseling to the patient. With these concerns in mind, the next section of this Article outlines the existing state and federal privacy law framework that the state and federal courts have applied to the disclosure, dissemination and use of patient prescription PHI.

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. Within that article, Brandeis and Warren outlined a common law individual right to privacy, which they characterized as a right “to be let alone.” 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.”

While Brandeis and Warren provided a general overview of the common law right to privacy, along with broad parameters for defining the right to privacy and corresponding remedies, the more concrete framework for a right to privacy was developed in 1960, when Dean William Prosser formally classified the four torts that generally 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. Dean Prosser’s classification was subsequently adopted in the 1977 Restatement (Second) of Torts, which many states have adopted as well. 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 and the breach of confidence tort, which is separate and independent from the privacy torts.

Along with tort actions for invasion of privacy or breach of confidentiality, the state-based right to privacy in PHI is also found within state constitutions and state privacy statutes. Regardless of the source of the privacy right, 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 information that they provide to their pharmacists. Similarly, in the context of unauthorized use of patient prescription PHI, a Massachusetts trial court recognized a cause 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. Likewise, the Rhode Island Supreme Court 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.

On the other hand, the Supreme Court of South Carolina held that a pharmacist does not owe a pharmacy customer a duty of confidentiality. 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.

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. The court based its decision on a Connecticut statute allowing 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 search warrant.

Other courts fall somewhere in the middle of the two extremes. The Supreme Court of Vermont held that individuals have an expectation of privacy in their pharmacy records, but also held that a warrantless inspection of the defendant’s pharmacy records were sufficiently limited by state law to render the inspection reasonable. The Supreme Court of Delaware held that a pharmacy employee’s disclosure of a patient’s prescription information may be correctly characterized as a breach of confidentiality claim, but also held that the same activity would not give rise to an invasion of privacy claim. The Court ruled that the former tort is focused on wrongful dissemination of private information, whereas as 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.\textsuperscript{102}

These state cases demonstrate a few important points. First, state courts vary widely in how strong they view a patient’s right to privacy within patient prescription PHI.\textsuperscript{103} Second, even when state courts recognize a strong privacy interest in patient prescription PHI, they still differ greatly in the law that they choose to apply – common law, statutory law or state constitutional law – and how they apply that law to protect privacy within patient prescription PHI.\textsuperscript{104} Third, there do not appear to be any state court cases which 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 within identifiable patient prescription PHI.

**B. The Federal Right to Privacy**

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\textsuperscript{105} federal statutes regarding health information privacy are the Health Insurance Portability and Accountability Act\textsuperscript{106} (“HIPAA”) and the Health Information Technology for Economic and Clinical Health Act\textsuperscript{107} (“HITECH Act”), and the two relevant federal regulations are the Privacy Rule\textsuperscript{108} and the Security Rule\textsuperscript{109}, both promulgated pursuant to HIPAA.

To briefly summarize this statutory/regulatory structure, 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.\textsuperscript{110} The applicable regulations define protected health information as “individually identifiable health
information”¹¹¹ and they define individually identifiable health information as a subset of an individual’s health information that is:

(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.¹¹²

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;

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; [and]

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.¹¹³
The Privacy Rule also permits limited uses and disclosures of protected health information, including, but not limited to disclosures to the patient and disclosures and uses related payment, treatment and health care operations.\textsuperscript{114}

The HITECH Act recently amended HIPAA in the following ways relevant to this article. First, under the HITECH Act, covered entities are required to notify affected persons and HHS when there has been a breach or unauthorized disclosure of unsecured protected health information.\textsuperscript{115} Unsecured protected health information includes all information that has not been rendered “unusable, unreadable, or indecipherable to unauthorized individuals,” either through encryption or destruction.\textsuperscript{116} Second, business associates of covered entities are now directly required to comply with HIPAA’s privacy and security requirements.\textsuperscript{117} 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.\textsuperscript{118} 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 the disclosure.\textsuperscript{119} Fifth, patients may request accountings of disclosure of their electronic protected health information over the three year period prior to the request.\textsuperscript{120} Sixth, covered entities and business associates are prohibited from selling protected health information without patient authorization, except for certain circumstances.\textsuperscript{121} 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.\textsuperscript{122}

Pursuant to the HITECH Act, HHS has issued a Notice of Proposed Rulemaking implementing the HITECH Act HIPAA modifications.\textsuperscript{123} There is no Final Rule yet, but the Proposed Rule proposes the following 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\textsuperscript{124}

Given the focus of this article on the use of encrypted or de-identified patient prescription PHI, it is necessary to highlight two particular provisions of the federal privacy statutes and regulations. 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 the Privacy Rule and open to dissemination without restriction.\textsuperscript{125} The Privacy Rule defines de-identified PHI as PHI for which “seventeen specific fields of data are removed or generalized.”\textsuperscript{126} The Privacy Rule also provides that PHI is only de-identified if “the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”\textsuperscript{127}

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.”\textsuperscript{128} HHS considers encrypted PHI to be “unusable, unreadable, or indecipherable to unauthorized individuals.”\textsuperscript{129} 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.”\textsuperscript{130}
Transitioning from federal statutory privacy protections to constitutionally-based privacy protections, the foundation for a constitutional right to privacy in health information originally came from Justice Brandeis’ dissent in *Olmstead v. United States.* In *Olmstead,* Justice Brandeis asserted the existence of a broad privacy right guaranteed by the constitutional amendments. In his dissent, Justice Brandeis incorporated the privacy concepts from his law review article almost forty years earlier, stating that the 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.”

Of course Justice Brandeis’ statement on a constitutional right to privacy was merely the beginning constitutional privacy jurisprudence, as the first Supreme Court controlling precedent acknowledging a right to health–related privacy arose almost forty years later in *Griswold v. Connecticut,* in which the Supreme Court held that state laws prohibiting the use of contraceptives violated a constitutionally based right to marital privacy. 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.”

Following *Griswold,* the Supreme Court expanded its right to privacy jurisprudence further into the health care arena in *Roe v. Wade.* 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.”

*Roe* focused on decisional privacy or the right to make certain personal decisions without government interference, whereas this Article focuses more on “disclosure privacy” or the
individual’s constitutional right to control the disclosure of his or her medical information. The Supreme Court’s first foray into “disclosure privacy” and privacy within medical information was the 1977 case, *Whalen v. Roe*, in which Justice Stevens, on behalf of the majority, upheld the constitutionality of a New York statute which 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 an unlawful market.” New York had enacted the statute as a way to monitor, investigate and enforce laws against prescription drug abuse.

Rejecting the privacy violation claim, the *Whalen* Court held that the New York statute did not pose a sufficiently grievous threat to the patient interest in avoiding public disclosure of one’s prescription drug use behavior or the interest in ensuring that patients will continue to obtain the prescription drugs that they need and not cease to do so because of the fear of public disclosure. 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.” As further justification for its holding, the Court also recognized that the state has broad police powers in regulating the prescription of drugs.

In the end, the *Whalen* Court ruled, on the facts of the case, 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. Nonetheless, the Court also recognized that increased computerization of health information in the future, particularly within centralized
databases, would allow medical records to be more easily accessed and heighten right to privacy concerns.  

*Whalen* was the Supreme Court’s last examination of the constitutional right to privacy within the context of PHI and prescription PHI and left unanswered whether or not patients have a right to privacy in prescription PHI. Since *Whalen*, various lower courts have looked at this issue, and within the context of health PHI and prescription PHI, there is “an unresolved circuit split as to whether there is a constitutional right to protection against disclosure of personal information.” It appears that nine circuits recognize a constitutional right to privacy in personal information, health or otherwise, while the Sixth Circuit reaches the opposite conclusion and the Eighth Circuit recognizes such a right only in instances involving egregious disclosure.

Looking at three of these Circuit Court rulings in more detail, in *Doe v. Southeastern Pennsylvania Transportation Authority* ("SEPTA"), the plaintiff, an employee of a public entity, SEPTA, filed a Section 1983 civil rights claim against SEPTA and his individual supervisor for invasion of privacy related to his employer and supervisor learning, through his prescription records, that he suffered from HIV. 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. The *SEPTA* Court reversed the jury verdict in favor of the plaintiff, holding 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. The Court characterized the employer’s privacy
intrusion to be minimal and held that SEPTA need not prove it had a compelling interest in obtaining the prescription information.\textsuperscript{154}

Similarly, in \textit{Douglas v. Dobbs}, the Tenth Circuit also 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.\textsuperscript{155} The \textit{Douglas} Court followed \textit{Whalen} in finding that the government has broad police powers to justify regulation of the prescription of drugs and certain privacy invasions with regard to prescription drug records.\textsuperscript{156}

Rounding out this trio of cases, in \textit{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.\textsuperscript{157} Following \textit{Whalen} and \textit{SEPTA}, the Court 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.\textsuperscript{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.\textsuperscript{159}

As demonstrated by the cases above and the Circuit Court split, the strength of a constitutional right to privacy in prescription PHI and what sort of constitutional scrutiny regulations of such a right engender are still somewhat open questions.\textsuperscript{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.”\textsuperscript{161} Even more unresolved is whether or not and to what extent patients have a federal right to privacy in de-identified prescription PHI, as there are no federal statutes and there appear to be no federal cases directly addressing this issue.
C. State Legislative Responses to Data Mining and Detailing

Before moving on to evaluating the options available for protecting the privacy of de-identified patient prescription PHI, it is important to examine the most recent direct attempt by three states at regulating the use of prescription data. Over the past five years or so, New Hampshire, Vermont and Maine, have each enacted statutes directed toward curtailing data mining of prescription information and the use of that information for detailing purposes. As will be discussed in more detail below, despite representing an effort to protect, to some extent, patient privacy in patient prescription PHI, these state statutes are more targeted at regulating data mining and detailing from the prescriber’s perspective rather than the patient 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 prohibits the license, transfer, use or sale of patient-identifiable and prescriber-identifiable prescription information for certain commercial purposes. Those commercial purposes include “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.” New Hampshire sought to ensure compliance with the PIL through various civil and criminal penalties, including subjecting violators to possible misdemeanor or felony prosecution, civil monetary penalties of up to $5,000 per violation, and/or misdemeanor or felony prosecution under New Hampshire’s unfair and deceptive trade practices law.
2. Vermont

Following New Hampshire’s passage of the PIL, in 2007, Vermont enacted a modified opt-in version of the New Hampshire law. In relevant part, the Vermont law provides that a pharmaceutical manufacturer, 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.” The statute defines the term “marketing” to:

[I]nclude 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.

The statute essentially prohibits using prescriber-identifiable information for marketing purposes, unless the prescriber agrees to or opts-in to such a use. A prescriber opts-in through his or her licensing applications or renewal forms and may revoke his or her opt-in at any time.

Along with its substantive provisions and procedural requirements, the Vermont law also provides for an enforcement scheme for violations. More specifically, the Vermont statute provides 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 is akin to a civil claim under Vermont’s consumer fraud act.

3. Maine

The third state to target prescription data mining and detailing was Maine, which in 2008 enacted an opt-out prescription drug information confidentiality law. The difference between
the Vermont opt-in approach and the Maine opt-out approach is that Vermont prohibits
marketing with the use of prescriber data unless the prescriber consents, whereas Maine allows
marketing with the use of prescriber data unless the prescriber opts for confidentiality protection.

The Maine law provides 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
defines “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 opts-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 Data miners and pharmaceutical companies are made aware of the
opt-out prescribers through public monthly updated lists “of all prescribers who have filed 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
D. The Data Mining Court Cases

As might be expected, all three of the state statutes outlined above have since been challenged in federal court on constitutional grounds. Perhaps reflecting the prescriber centric focus of the statutes being challenged, all three of the Circuit Court decisions have focused more on data mining and detailing from the prescriber perspective as opposed to the patient 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.

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 miner companies’ challenge to the New Hampshire PIL on grounds that the law infringed upon their free speech and violated the Commerce Clause. In *Ayotte*, a split panel of the First Circuit, held that the PIL regulated conduct and not speech, thereby being entitled to more lax constitutional scrutiny. The Court ruled that even though data can take the form of protected speech, the 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. The Court reasoned that the PIL did not eliminate speech, as such, but, rather eliminated “the detailers’ ability to use a particular informational asset – prescribing histories – in a particular way.”

To the extent that the PIL regulated any speech, the Court further ruled that such speech was of little societal value and any information exchanges prohibited by the PIL were not “the sorts of exchanges valued by the Supreme Court’s First Amendment jurisprudence.” The Court reasoned that the PIL-limited exchange of data between data miners and the
pharmaceutical companies was not the type of exchange valued under the First Amendment because the prescribed exchanges were “undertaken to increase one party’s bargaining power in negotiations.”

Despite finding that the PIL regulated conduct and not speech, the Court alternatively held that to the extent that the PIL regulated speech it regulated commercial speech. Accordingly, the Court applied the *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York* test for commercial speech, which provides that government restrictions on commercial speech are permissible provided those restrictions directly advance a substantial governmental interest and restrict speech no more than is necessary to further that interest. The Court ruled that the PIL goal of containing health care costs was a substantial government interest.

Turning to whether or not the PIL directly advanced that government interest, the Court held that 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.” 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.”

Moving to the third prong of the *Central Hudson* test, the Court ruled that there existed no alternative legislative approaches which would have achieved the goals of the PIL without restricting speech. Rejecting possible alternatives, the Court ruled that banning free drug samples would harm indigent patients, that 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 that 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.\textsuperscript{191}

Having resolved the First Amendment speech issue, the Court’s final ruling addressed the data miners’ claim that the PIL violated the Dormant Commerce Clause because the PIL failed to include a geographic limitation and directly regulated out-of-state transactions between data miners selling prescription data to pharmaceutical manufacturers.\textsuperscript{192} The Court rejected this argument, instead presuming that the 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.”\textsuperscript{193}

Notably, the \textit{Ayotte} Court avoided any detailed discussion of patient privacy interests within the context of the PIL, although the Court acknowledged that the PIL asserted that patient privacy was a substantial government interest for purposes of a commercial speech analysis.\textsuperscript{194} Similarly, the concurring/dissenting opinion also avoided discussing patient privacy implications of the PIL, reasoning that the plaintiffs did not challenge the statute’s restriction on the use of patient-identifiable prescription information.\textsuperscript{195}

2. IMS Health, Inc. v. Mills

Following the \textit{Ayotte} decision, the First Circuit issued a similar ruling with regard to three data miners’ challenge to the Maine prescriber confidentiality law.\textsuperscript{196} Finding the data miners’ legal challenge and the Maine statute to be very similar to the challenge and statute at issue in \textit{Ayotte}, the Court relied upon \textit{Ayotte} in holding that the Maine “statute regulates conduct, not speech, and even if it regulates commercial speech, [the statute] satisfies constitutional standards.”\textsuperscript{197}
In addition to relying on Ayotte, the Court, in applying the Central Hudson test, also ruled that assuming the Maine law regulates commercial speech, then unlike Ayotte the Maine statute, through its opt-in provision, “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.”

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.

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. Moreover, the Court ruled that the Maine law’s opt-in mechanism, by definition, was a least restrictive means of protecting prescribers’ privacy interests. 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.

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 to 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.” 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] does not risk imposing regulatory obligations inconsistent with those of other states.”

Alternatively, in finding no violation of the Commerce Clause, 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. The Court held that Maine was able to demonstrate that the law creates substantial in-state benefits for Maine prescribers who want to avoid unwanted targeting. On the other side of the ledger, the Court ruled 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 Maine law would prove insubstantial, given that they need only ensure that they avoid using or selling opted-in Maine prescriber data.

As in the Ayotte case, the majority, along with concurring opinion, 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 government interest within the context of the commercial speech analysis of the Maine statute.

3. IMS Health, Inc. v. Sorrell

The third case in the trio of cases challenging the state data mining statutes is 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. 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. 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. 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.” In ruling that the Vermont statute regulated speech, the Court also held that the regulated speech was commercial as opposed to noncommercial speech because “the primary purpose of detailing is to propose a commercial transaction—the sale of prescription drugs to patients.”

Having found that the Vermont statute regulated commercial speech, the Court then analyzed the statute under the *Central Hudson* test. 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. 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.” 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.

Focusing on whether the Vermont statute directly advanced the state interest in reducing health care costs and protecting public health, the Court ruled that the statute only indirectly promoted those interests because it failed to directly restrict prescribers’ prescribing practices and/or restrict detailers’ marketing practices. 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. 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.

Along with finding that the Vermont statute failed to survive intermediate scrutiny because it indirectly promoted the state’s interests, the Court also ruled that those governmental interests could have been fulfilled in a less speech restrictive manner. The Court ruled that the Vermont statute was overly burdensome because it promoted fewer prescriptions of all brand name prescription drugs, which was a poor fit with the legislative goal of restricting overprescribing of only “new and allegedly insufficiently tested brand-name drugs in cases where there are cheaper generic alternatives available.” 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.” 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.

Unlike the Ayotte and Mills cases, the Sorrell Court indirectly addressed 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 government interest to justify the state’s regulation on commercial speech.
The Dissent also addressed the government interest in patient privacy and, contrary to the majority, opined that patient privacy was a substantial government interest worthy of protection under the Vermont statute. 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 “rampant dissemination of confidential information.” 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.

4. The Path Forward

Ayotte, Mills and Sorrell are not the end of the story for the New England data mining statutes. In early 2011, the Supreme Court granted a writ of certiorari in the Sorrell. Regardless of which side of the Circuit split the Supreme Court follows, the issue of protecting the privacy of patient prescription PHI will remain an ongoing concern. Obviously, if the Supreme Court finds the Vermont statute to be unconstitutional, then other alternatives must be explored to protect patient privacy in patient prescription PHI. Alternatively, if the Supreme Court upholds the constitutionality of the Vermont statute, only Maine, Vermont and New Hampshire, have passed legislation restricting the use of prescription information and only within the context of data mining and detailing. Moreover, from the patient privacy perspective, there are weaknesses within these existing state statutes that could be strengthened in future legislation regulating the disclosure of patient prescription PHI, as discussed infra.

IV. Evaluating the Alternatives for Protecting Patient Prescription Information Privacy

Reviewing federal and state statutes, ethical codes, state common law and federal constitutional law, one may argue that there are at least five available options in existence, which serve to protect patient prescription information privacy. This section seeks to examine each of
these five options. While some of these options may seem promising, each of them suffer from weaknesses that prevent them from being an optimal solution for protecting either identified or de-identified patient prescription PHI.

A. The New England State Data Mining Statutes

Assuming the upcoming Supreme Court decision in Sorrell supports the constitutionality of the Vermont, New Hampshire and Maine statutes described above, these three statutes are the best starting point for examining available alternatives for protecting patient prescription information privacy. Facialy these statutes would appear to be directly on point in protecting the privacy of patient prescription PHI, but they actually suffer from a number of flaws in terms of their effectiveness in achieving this goal.

The New Hampshire and Vermont statutes are woefully inadequate in even addressing patient privacy interests, particularly privacy interests in de-identified patient prescription PHI. The New Hampshire statute only protects the privacy of patient identifiable information and says nothing about de-identified or encrypted patient information.\textsuperscript{230} Whereas, the Vermont statute evinces the intent to protect the privacy of prescription information\textsuperscript{231}, but never mentions a method for protecting patient prescription PHI and focuses entirely on protecting prescriber identifiable information.\textsuperscript{232}

In contrast to the New Hampshire and Vermont statutes, the Maine statute is the statute that comes closest towards 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].”\textsuperscript{233} 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. A court may easily find that indirectly identifiable information is not the same as de-identified or encrypted information.

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. Any other individual and/or entity, including drug manufacturers or researchers, can use prescription information for marketing, or other purposes for that matter, without violating the statute. Under the Maine statute, a pharmacy could lawfully sell or transfer the patient prescription information directly to a pharmaceutical manufacturer for marketing purposes.

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. While some patients may consider marketing to be the most pernicious use of prescription information and the only use for which they want their privacy protected, other patients may legitimately want the privacy of their prescription information protected from being used in other contexts, such as for research purposes.

The New Hampshire and Maine statutes are also too narrow in how they protect prescription information privacy. Unlike the Vermont statute, neither of them directly regulates the marketing of prescription information. Rather, the two statutes place the burden on pharmacies, data miners, insurers and similar entities not to transfer the prescription information to downstream marketers, when the transfer will result in using the information for marketing purposes. 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. How the state would discover violations and enforce the prohibition against downstream marketing is far from clear.

Turning to the opt-in and opt-out provisions in the Vermont and Maine statutes, a major concern with both statutes is that they only allow prescribers to register for confidentiality through licensing and renewal applications. Accordingly, there are only limited opportunities during limited time periods for prescribers to assert their rights to prescription information confidentiality. The opt-in and opt-out processes also fail to incorporate a real time aspect to them, which weakens their effectiveness. For example, the Maine statute only requires monthly updates to the list of prescribers seeking confidentiality protection under the statute. 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. 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. 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.

Even if the three statutes are sufficiently patient privacy centric, they still lack vigorous compliance and enforcement provisions. When statutory violations occur under the three statutes, it is 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 patient to continue using drug “x,” or direct marketing materials soliciting the patient to switch a similar competitor drug, drug “y.” A patient may rightfully 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, but do so in a sufficiently vague manner. 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 or not the drug manufacturer used that patient’s prescription information to target or solicit him or her.

Patients will also have no way of knowing whether their prescription information was used by drug manufacturers to detail their prescribers. If a drug manufacturer merely uses the prescription information to target particular prescribers, then savvy marketing will prevent the prescriber from knowing that his or her prescriber information was used for targeting purposes, let alone the patient knowing. Similarly, if a drug manufacturer uses prescription information to develop a more effective marketing message without directly soliciting the prescriber with that prescriber’s own prescribing information, then not even the prescriber will be aware of that a statutory violation has occurred. In fact, the Dissent in Sorrell noted that detailers are prohibited from directly referencing a prescriber’s prescription data during detailing sessions.\textsuperscript{246}

There is simply a lack of 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 will become aware of breaches of prescription information privacy. There is nothing within the state statutes to require
pharmaceutical manufacturers to publish to the world how they design their marketing campaigns or what information they use to design them, and none of the three statutes prohibit pharmaceutical manufacturers from directly marketing to prescribers or patients. 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.

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 in protecting patient privacy.

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. 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 three years, which can be extended if the prescriber re-registers. 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.

Following the AMA’s promulgation of the PDRP, PhRMA revised its professional code, the PhRMA Code, to track the provisions of the PDRP. The PhRMA Code announced a
commitment by PhRMA to address its own marketing practices to prescribers in an attempt to impact marketing practices that might be perceived as inappropriate by patients.\textsuperscript{251} Despite this commitment, the PhRMA Code only addresses ethical uses of prescriber data, not patient data, and, in fact, condones any “responsible” use of patient data, provided such data de-identifies patients.\textsuperscript{252} Moreover, as with the AMA PDRP, the PhRMA Code weakly relies on discretionary and voluntary compliance for enforcement.\textsuperscript{253} However, most troubling is the fact that PhRMA’s Code is “promulgated by lobbyist groups within the industry, leaving the neutrality of these guidelines highly questionable.”\textsuperscript{254}

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, which 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.”\textsuperscript{255} 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.\textsuperscript{256} 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.\textsuperscript{257} 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.\textsuperscript{258} 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 and/or other entities. 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 confidentiality, in the chain drug store context, is only as strong as the pharmacy employer’s respect for that confidentiality.

In summary, the ethical codes that govern the privacy of patient prescription PHI, like the New England data mining statutes, are much 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 effective 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. Accordingly, relying upon state-based statutory protections results in patients in different states having potentially different levels of privacy protection in their prescription records, entities subject to patient prescription privacy regulation bearing the cost and burden of complying with potentially 50 different statutes and entities that transmit prescription PHI interstate having to figure out which state’s rules apply and when. 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.

Second, the right to privacy embodied within state common law and the Restatement is non comprehensive and provides only modest privacy protection. State privacy tort actions
apply in a narrow range of highly qualified circumstances, which 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.’” 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.”

In the context of a patient-pharmacist relationship, the privacy torts further fail to provide adequate protection because the privacy torts and breach of confidence tort usually require patients to demonstrate a special relationship between the patient and the pharmacist disclosing the patient’s private information. However, pharmacy patients cannot demonstrate such a relationship or such an expectation of privacy therein because states do not recognize a special relationship between a patient and pharmacist in contrast to the patient-physician relationship.

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

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. Many state statutes address narrow, specific informational privacy issues and are “riddled with exceptions.” 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.274

Fourth, state constitutional privacy protections have rarely been invoked to protect informational privacy, such as the privacy of patient prescription PHI.275 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 and 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 for that matter.276 In order to state a constitutional right to privacy claim, a plaintiff must allege that a state actor violated that plaintiff’s right to privacy.277 Under the state actor doctrine, the Supreme Court has held that the deprivation of the constitutional right – in this case the right to privacy – must be “fairly attributable to the State.”278 The deprivation must be by a state official, be done in concert with or with significant aid from a state official or must be “otherwise chargeable to the State.”279

While the transfer of patient prescription PHI to law enforcement agencies or government entities for public health purposes may meet the state action test, to the extent such transfers are
required by law, the holding in *Whalen* probably forecloses any such claim.\textsuperscript{280} Even if such claims are viable in the law enforcement and public health context, 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, as within the context of those two lawsuits CVS Caremark appears to be acting as a private entity.\textsuperscript{281} The state actor 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, and therefore constitutional privacy claims with regard to such information are unlikely to meet the state actor test.\textsuperscript{282}

The constitutional protection afforded to health information is also too narrow to adequately protect the privacy of patient prescription PHI.\textsuperscript{283} To meet constitutional privacy standards, the health information to be protected must be both subjectively and objectively private, rather stringent standards.\textsuperscript{284} Even if identifiable patient prescription PHI is deemed to be both subjectively and objectively private, which is still an open question as outlined above, de-identified patient prescription PHI is even less likely to be deemed by a federal court to be subjectively and objectively private, in light of the fact that 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 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. 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, with more expanded application to business associates of these entities. For example, pharmaceutical companies are not usually covered entities under HIPAA.

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. There are too many ways in which patient prescription PHI can be used and disclosed without violating HIPAA under the guise of payment or health care operations. The CVS Caremark lawsuits are based upon allegations that demonstrate how entities can share, disclose and disseminate patient prescription PHI in such a manner as to avoid potential HIPAA violations.

Lacking a patient proactive focus, HIPAA also fails to require consent for the use of protected health information for certain purposes, such as payment, treatment and health care operations. Again, the allegations within the CVS Caremark lawsuits illustrate how certain entities use the HIPAA health care operations exception to disclose private medical information without violating HIPAA. Even outside of treatment and billing, there are many HIPAA permitted unrestricted uses of patient prescription PHI, which do not require patient consent, particularly by secondary users. 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.
Even more significant within the context of this Article, the Privacy Rule expressly excludes from its privacy protections de-identified health information. 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.

HIPAA’s de-identification standards are also open to criticism. Even though HIPAA may consider a document containing health information to be de-identified, that does not mean that such a document is actually de-identified or rendered absolutely incapable of re-identification. HIPAA considers data to be de-identified if certain patient identifying information is removed, such as name, address and social security number. However, HIPAA does not require other information, such as height, weight, ethnicity, birth year and 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.

Since the New England data mining cases also describe the prescription information used by data miners and pharmaceutical manufacturers as encrypted, as well as de-identified, it is also important to look at how the HIPAA regulations treat encrypted health information. 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 of a confidential process or key.” The Security Rule also requires covered entities, and in the future business associates, to safeguard electronic PHI through encryption or a comparable method.

Once PHI is encrypted, HHS considers such information to be adequately protected from disclosure, as it considers encrypted PHI to be “rendered unusable, unreadable, or indecipherable
to unauthorized individuals.“ In fact, in HHS’ Interim Final Rule regarding notification of breaches of PHI, HHS explained that if a covered entity encrypts PHI, pursuant to the Security Rule, and later discovers a breach of that encrypted information, it need not even provide breach notification to the patient. In other words, the breach notification requirements only apply to breaches of unsecured protected health information. HHS does not appear all that concerned with using HIPAA to force covered entities to notify patients of breaches of the privacy involving encrypted PHI, let alone 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. As an example of an application of this principle, if a patient plaintiff jointed one of the CVS Caremark lawsuits, he or she would be 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. This enforcement scheme sends the wrong message that patient prescription data privacy rights “belong to the healthcare system and not to patients.”

Related to enforcement is the question of effectiveness and whether HIPAA is truly effective. One study indicated that there were 291 publicly reported health information data breaches from 2003 through 2007, which potentially exposed the health information of more than 16 million patients. With medical information privacy breaches over a four year period potentially impacting 16 million or more patients, one has to ask whether HIPAA goes far
enough in protecting patient information privacy. There are doubts “as to the level of the federal government’s commitment to the enforcement of the HIPAA rules.”

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

V. Guiding Principles for Federal Legislation to Protect the Privacy within Encrypted or De-Identified Patient Prescription Information

Reviewing the available options above, existing state and federal privacy protections fail to vigorously protect patient privacy in encrypted or de-identified prescription PHI. To summarize some of the weaknesses outlined above and which future federal legislative efforts must address, first, across all of the options there is an insufficient focus on protecting the privacy of de-identified or encrypted prescription PHI and not just identifiable prescription PHI. Second, with regard to the New England statutes and other state-based options, there are Commerce Clause concerns, and more generally, practical concerns regarding a lack of national uniformity in protecting de-identified or encrypted patient prescription information privacy. Third, the New England statutes and the ethical options are more prescriber centric in their focus than patient centric. Fourth, in the case of the New England statutes, the ethical options and HIPAA, patients lack the power to control the privacy of and disclosure of their de-identified or encrypted prescription PHI. Fifth, there are compliance weaknesses across most, if not all, of the available options.

In light of these concerns, any future statutory attempt to regulate prescription PHI, be it federal or state, must address the lack of protection that patients currently have in guarding the
privacy of their de-identified or encrypted prescription PHI. Patients have a legitimate interest in protecting the privacy of their de-identified or encrypted patient prescription PHI because such information still provides intimate details about a patient’s life and health. Moreover, de-identified information can all too easily be re-identified and encrypted information can all too easily be decrypted. 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.

Moving on to whether state or federal legislation is preferable, while the upcoming Supreme Court decision in *Sorrell* will resolve the Commerce Clause issue posed by the New England statutes one way or the other, any future efforts to provide protection for de-identified or encrypted patient prescription PHI should be federal. Even if the Supreme Court finds the Vermont statute to be Constitutional, a federal privacy statute, as opposed to state-based privacy statutes, offers a better way to protect the privacy of de-identified or encrypted patient prescription PHI.

From a practical perspective, a federal statute provides a valuable level of uniformity in privacy protection. For example, in light of the state causes of action within the two CVS Caremark lawsuits, it is possible that the two different courts, applying two different sets of laws, may come out on opposite sides on whether CVS Caremark’s alleged prescription information sharing scheme, which is the same for both lawsuits, raises privacy concerns. The end result is confusion, uncertainty and inconsistency regarding whether the CVS Caremark alleged information sharing scheme is lawful or not.
With a federal statute, every patient, regardless of where he or she lives, has the same level of privacy protection for his or her de-identified or encrypted prescription PHI. Without a federal statute, a patient living in one state could have his or her de-identified or encrypted prescription PHI subject to a high level of protection in one state, then change residence to a different state, without such protections, and suddenly lose all of the protection. Similarly, a person could live near a state border and fill prescriptions at different pharmacies in different states, with resulting differing levels of privacy protection. Under these scenarios, the privacy of an individual’s prescription PHI is only as strong as the privacy guaranteed by the state with the weakest privacy provision.

On the other side of the ledger, a federal statute is beneficial to those who would use de-identified or encrypted patient prescription PHI because they would not need to comply with potentially fifty different privacy statutes. A federal, as opposed to state-based, privacy statute would be much less onerous and burdensome on those required to comply with it. For example, a federal statute would provide a level of clarity for CVS Caremark, in the context of the two CVS Caremark lawsuits, 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.” Today, computerized and internet-based information can be accessed across state lines from remote locations, such that 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.

A state statute would also raise enforcement concerns not applicable with regard to a federal statute because of jurisdictional limits and states’ weak enforcement abilities. It is
very difficult to enforce in-state violations committed by out-of-state violators, as illustrated by the New England data mining cases.\textsuperscript{321}

With a federal statute being more appealing than a state statutory option, the scope of federal preemption is an issue that must 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 those who use prescription data may be subject to potentially different standards and burdens, at least with regard to states who implement more strict prescription privacy statutes than the federal law.\textsuperscript{322} Accordingly, in terms of simplification, efficiency and potential cost savings, a federal law that is completely preemptive of state law is the preferable approach.

Along with being a federal statute and specifically encompassing de-identified or encrypted patient prescription PHI, any future statute should also be more patient centric, unlike the New England and the ethics-based options. Both sets of options demonstrate a greater concern for how data miners and pharmaceutical companies use prescriber prescription information, as opposed to a concern for how such entities and others use patient prescription PHI.\textsuperscript{323} The protections encompassed within both alternatives seek to empower prescribers to prevent the disclosure, dissemination and use of their own information, and not necessarily the patient’s prescription PHI. Therefore, future legislative efforts to protect de-identified or encrypted 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 expressly 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 protect the privacy of de-identified or encrypted patient prescription PHI. 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 and is focused more on notice to the patient regarding use of such information, rather than patient consent for such use. The federal constitutional options and state-based options really only provide reactive privacy protection, meaning these options do not empower patients to prevent unauthorized access to their prescription PHI, but only allow for them 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. While *The Muecke Company, Inc.* Complaint seeks injunctive relief, the focus of the two CVS Caremark lawsuits is really on privacy breaches of patient prescription PHI that have already occurred.

Future legislative efforts to protect the privacy of de-identified or encrypted patient prescription PHI must empower the patient a priori to choose if or how his or her prescription information will be used. While this may be accomplished in any number of ways, 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, which allows the patient to opt-in to protect the privacy of his or her identifiable, de-identified and encrypted prescription information. The 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 or 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.

A few points require elaboration or clarification. First, even though the use of identifiable prescription information is already restricted under many situations\textsuperscript{330}, 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 avoid HIPAA requirements and lawfully share patient prescription PHI.\textsuperscript{331} Nonetheless, many patients may still object to the manner in which CVS Caremark is alleged 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 still may 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 some purposes, but not for other purposes. Ideally, more choice provides more empowerment for patients. However, tracking many different categories of use of prescription information for compliance and enforcement purposes would probably be a logistical and burdensome nightmare.

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.\textsuperscript{332} Equally so, health care providers have a legitimate need to gain access to prescription information as part of treating a patient.\textsuperscript{333} Finally, as established under \textit{Whalen} and \textit{Citizens}, there are strong policy reasons to allow for the sharing patient prescription PHI for law enforcement and public health purposes.\textsuperscript{334}

Enforcement is another area of weakness within existing alternatives for protecting the privacy of de-identified and encrypted patient prescription PHI. Accordingly, it is important that future legislative efforts ensure that enforcement of patients’ privacy wishes be strong and effectively deter violations of the statute. As discussed within the context of the New England statutes, the unusual enforcement mechanisms and attempt to indirectly regulate downstream marketing allows data miners and pharmaceutical manufacturers to potentially use patient prescription PHI in an unlawful manner without discovery by the patient or state.\textsuperscript{335} Moreover, under HIPAA, enforcement is entirely within the control of HHS, which has demonstrated weak enforcement in the past.\textsuperscript{336}

To remedy these enforcement weaknesses, future legislative action to protect the privacy of de-identified or encrypted 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.\textsuperscript{337} If a person can track a FedEx package as it moves across the world, there is no reason why software could not be developed to allow a patient to track his or her prescription information. A patient should be able to use a code assigned to his or her
prescription information to allow that patient to track that information online wherever it goes.\textsuperscript{338} Such patient empowerment should increase deterrence of violations of prescription privacy.

Admittedly, this tracking system is not a perfect system. There are weaknesses. First, such a system would probably be expensive and burdensome for the government, pharmacies, data miners, pharmaceutical manufacturers and others who might use patient prescription PHI to implement. Second, the system might be difficult for low income patient populations, vulnerable patient populations and non-computer savvy patients to use. Third, the software or tracking system would have to be secure or else there would be a high risk of hacking.\textsuperscript{339} Fourth, by attaching a code to de-identified or encrypted patient information, for purposes of tracking, one actually creates a risk of re-identification.\textsuperscript{340} The patient’s code is associated with that patient and raises a risk that that patient could be identified in relation to a particular set of prescription information if someone breaks the code. However, this latter concern may not be so great, assuming the code is only circulated among those entities who would have access to the patient’s identifiable prescription information anyway, such as a PBM or treating health care provider.

The tracking system in and of itself is not sufficient to deter violations. For more effective deterrence, HHS should conduct audits of the tracking system.\textsuperscript{341} HHS should be able to audit the tracking systems used by pharmacies, their headquarters, insurance companies, PBMs and related entities 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 such information for payment or treatment purposes.\textsuperscript{342} When HHS discovers violations, it should be empowered and encouraged to impose heavy civil monetary penalties on violators. Only strong enforcement of such penalties and sufficiently heavy penalties will bring about effective deterrence.\textsuperscript{343} Even so, to make deterrence
even more effective, patients should also be empowered to file a statutory cause of action against violators, along with a set dollar value statutory damage amount per violation. Combined, the HHS and patient enforced deterrence should place an adequate check on entities that may wish to violate the statute in the hopes that they will not get caught.

On a final note, any analysis of future legislative efforts to protect identifiable, de-identified and encrypted patient prescription PHI must also address the First Amendment issues raised within the three New England cases. Any legislation that seeks to protect the privacy of patient prescription PHI will simultaneously limit the use of that information, uses which in at least some cases may involve First Amendment commercial speech. As with the Commerce Clause issue, the upcoming Supreme Court decision in Sorrell will likely provide valuable guidance on whether the type of legislation contemplated within this Article would pass First Amendment muster. Nonetheless, it is worth briefly addressing how the statute envisioned here would fare under a Supreme Court commercial speech analysis.

In comparing the statute envisioned here with the three New England state statutes for commercial speech analysis purposes, there positives and negatives to the contemplated statute in terms of surviving constitutional scrutiny. On the upside, the substantial government interest to be protected under the contemplated statute is the government’s interest in protecting a patient’s right to privacy in patient prescription PHI, including de-identified and encrypted prescription PHI. The strength of this patient privacy interest should be much stronger than the prescriber’s privacy interest in his or her prescription history, as highlighted within the context of the New England data mining cases. Many federal courts have recognized the former to be a constitutionally guaranteed right, albeit a non-absolute right. The same cannot be said as to the existence of a prescriber 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. Accordingly, the patient’s right to privacy should carry more weight under a commercial speech analysis than the prescriber’s claimed right to privacy in the New England data mining cases.

This leads to the next issue of whether or not the statute envisioned in this Article would promote a substantial government interest in patient privacy and whether it would be narrowly tailored enough to pass constitutional muster. The former should be self-evident, but the latter is a much more difficult question. The three New England statutes narrowly limit the use of patient prescription PHI in the field of marketing, whereas the statute envisioned in this Article allows patients to opt-in to protecting all uses of their prescription information, except for payment, treatment, law enforcement and public health purposes. Accordingly, the argument that the statute envisioned in this Article is narrowly tailored to protect patient privacy may not be as strong compared to the narrow tailoring analysis of the New England statutes.

Still, it is difficult to conceive of how one could protect a patient’s constitutional right to privacy in a narrower manner than to allow a patient to opt-in to privacy protection for all purposes except those that are necessary and/or serve important policy goals, such as payment, treatment, fraud, drug abuse detection, law enforcement, and public health. The New England data mining statutes have the ability to narrowly focus on regulating drug marketing and still fully protect prescriber privacy interests because prescribers impacted by those statutes are concerned only with privacy as it relates to the use of their prescribing information for marketing purposes. Patients, on the other hand, may deem any disclosure of their identifiable, de-identified or encrypted prescription information for a variety of purposes, in addition to marketing, to be a breach of their privacy. Unlike the prescribers’ concerns in the New England
data mining cases, patients’ concerns regarding the privacy of their prescription information is wider in scope, which thereby requires a privacy protection statute that is wider in scope. Given the wide scope of patients’ interests in protecting the prescription information, the best effort to design a statute as narrowly tailored as possible is to include the opt-in check box concept outlined above. Such opt-in concepts are often deemed to be narrowly tailored per se.\(^{350}\)

As part of the narrow tailoring analysis, it is also notable that unlike the cases involving the New England statutes a challenge to the statute envisioned by this Article would pit two constitutionally guaranteed rights against each other. A data miner or pharmaceutical manufacturer challenging the envisioned statute would probably claim that the envisioned statute violates that entity’s commercial speech rights, as with the challenges against the New England data mining statutes. At the same time, the envisioned statute would exist to in order to provide protection for another constitutional right, the patient’s constitutional right to privacy in medical information. The result is that the envisioned statute embodies a conflict between the patient’s right to privacy and the prescription information user’s right to free speech.

Though not identical, an analogous conflict of constitutional rights has arisen previously in the pharmacy field within the context of pharmacist conscience laws, which protect pharmacists from being compelled to dispense contraceptive drugs to patients.\(^{351}\) Such conscience laws create a conflict between a pharmacist’s right to free exercise of religion and 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.\(^{352}\) Scholars have been split as to which right should prevail within the context of the conscience laws\(^{353}\), thus demonstrating the difficulty in determining which constitutional right prevails when two constitutional rights conflict head-to-head. Not surprisingly, it is difficult to anticipate whether a
pharmaceutical company’s right to free speech in the context of detailing outweighs the patient’s right to privacy in his or her prescription information or vice versa. Notably, neither right is an absolute right, such that either may be subject to regulation under certain circumstances.\(^\text{354}\)

Despite the difficulty in trying to predict which constitutional right will prevail, all in all, within the context of the envisioned statute, the patient’s right to privacy in prescription PHI should prevail over any detailers’ commercial speech claim. Generally, courts have allowed patient prescription privacy rights to be curtailed in only limited circumstances where there are very strong government interests at stake, such as law enforcement\(^\text{355}\) or drug abuse concerns.\(^\text{356}\)

By contrast, a private third party’s interest in access to an individual’s private medical information for purposes of marketing and profit making hardly rises to a level of importance equal to the government’s interest in public health or law enforcement. Moreover, in the past, when privacy rights and commercial speech rights “have come into conflict, privacy has traditionally won, easily passing intermediate scrutiny.”\(^\text{357}\)

A couple of other reasons are also worth mentioning as to why the envisioned statute will probably survive constitutional scrutiny within the context of a commercial speech analysis. First, as David Orentlicher has argued, to the extent that commercial speech is being regulated under the envisioned statute, the government should have more leeway in restricting such speech where data mining and detailing using patient prescription PHI has a negative impact on the public fisc.\(^\text{358}\) When detailing unnecessarily drives up drug spending and government programs, such as Medicaid, incur those costs, the government is indirectly footing the bill for that commercial speech and should have greater freedom to regulate such speech.\(^\text{359}\)

Additionally, the statute does not prohibit pharmaceutical manufacturers from communicating truthful information to prescribers through marketing.\(^\text{360}\) Under the envisioned
statute, pharmaceutical manufacturers can still market their drugs to and educate prescribers and the general public, but they cannot use certain patient designated prescription PHI in doing so. Moreover, as long as pharmaceutical manufacturers are allowed to continue to pitch their products to prescribers and the public, which they could do under the envisioned statute, then their strong profit motives and substantial profits will likely overcome any chill on commercial speech caused by the proposed prescription privacy statute.\textsuperscript{361}

VI. Conclusion

This Article has demonstrated that existing options for protecting the privacy of patient prescription PHI are simply not comprehensive and are inadequate. 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 HIPAA, fail to focus on the patient, as in the case of professional ethical codes, and/or are completely reactive in their approach, as in the case of the federal and state causes of action available for breaches of privacy and/or confidentiality. Even if the 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. Accordingly, patients seek and need a comprehensive federal statute to uniformly protect the privacy of both identifiable patient prescription PHI and de-identified or encrypted patient prescription PHI.

In developing a comprehensive federal statute, Congress has many options available for how to structure such a statute. However, for maximum effectiveness, any future federal statute should specifically protect the privacy of de-identified and encrypted patient prescription PHI, as well as identifiable patient prescription PHI, completely preempt state law, be patient centric, provide for a tracking provision and provide for strong, meaningful enforcement. It is important
to empower patients with the confidence that the information that they provide to their pharmacists remains as confidential and private as they wish, whether such information is identifiable, de-identified or encrypted.

1 Rockwell, 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 (Spring 2006) (discussing a survey which 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. Pharmacy & L. 127, 128, 130 (1992/1993) (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, 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 (Summer 2001) (arguing that as the use of computer technology grows, so does the risk to the privacy of medical records).
4 IMS Health, Inc. v. Sorrell, 630 F.3d 263, 266 (2nd Cir. 2010) (demonstrating a focus on Vermont statute’s restriction on the sale, use or transmission of prescriber-identifiable prescription data in finding the statute to be unconstitutional); IMS Health, Inc. v. Mills, 616 F.3d 7, 12 (1st Cir. 2010) (upholding Maine prescription privacy statute as a statute enacted to protect prescribers’ data privacy); IMS Health, Inc. v. Ayotte, 550 F.3d 42, 45 (1st Cir. 2008) (focusing on New Hampshire statute’s restriction on transfers of prescriber histories in upholding New Hampshire statute designed to prohibit transfers of prescription data with certain prescriber history information).
8 Schawbel, supra note 3, 909 (contending that “every day millions of individuals volunteer personal information in order to receive the benefits of health care”).
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).

Mowery, supra note 2, 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, 909 (arguing that individuals who volunteer personal information rarely question who can access that information and for what purposes); Ward, supra note 5, 75 (arguing that Americans value their privacy in prescription records, particularly when such information is used for purposes other than diagnosis or treatment).

Schawbel, supra note 3, 909.

Id.

Sorrell, 630 F.3d at 268 (describing the purchasers of prescription information data from data miners); Mills, 616 F.3d at 16 n. 4 (describing the entities to which data miners sell or license prescription information databases); Schawbel, supra note 3, 918 (describing the variety of entities seeking access to patient prescription drug data).

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).

Terry, supra note 6, 3 n. 8 (identifying the growing impossibility of de-identification as the greatest challenge to the de-identification model).

Id. (discussing the risk or re-identification of de-identified data); Robert Gellman, The De-identification Dilemma: A Legislative and Contractual Proposal, 21 Fordham Intell.Prop. Media & Ent. L.J. 33, 34-35 (2010) (arguing that “de-identification does not always make re-identification of individuals impossible”); Porter, supra note 6, 3 (discussing how publicly available auxiliary information may be used to re-identify anonymized information).

Porter, supra note 6, 3.

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

Id.

Id.

Terry, supra note 6, 3 n. 9.

Gellman, supra note 16, 34-35.

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

Porter, supra note 6, 3.

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).


Id. at 78 (describing how the cipher or key renders plaintext unreadable gibberish).


Northwestern 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).


Mark Lebovitch & Laura Gundersheim, “Novel Issus” or a Return to Core Principles? Analyzing the Common Link Between the Delaware Chancery Court’s Recent Rulings in Option 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).


Id. at ¶¶46, 48, 70, 77.

Id. at ¶¶52-55, 63.

Id. at ¶¶3, 77-81.

Id. at ¶¶3, 56, 65-67, 69, 77.

*Id.* at ¶¶1-9.

*Id.* at ¶29.

*Id.*

*Id.* at ¶¶34-36.

*Id.* at ¶32

*Id.*

*Id.* at ¶33.

*Mills*, 616 F.3d at 16 (describing the transfer of prescription data from pharmacies to data miners); *Klocke*, *supra* note 6, 512 (describing the data mining process as increasingly involving the purchase of patient prescription data from hospitals and insurance companies).

*Sorrell*, 630 F.3d at 267; *Mills*, 616 F.3d at 16; *Ayotte*, 550 F.3d at 45.


*Mills*, 616 F.3d at 16 (describing how data miners develop a complete picture of prescribers’ prescribing history); *Ayotte*, 550 F.3d at 45 (describing the scope of the industry in aggregating prescriber data as mind-boggling).

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

*Id.* at 46-47 (describing the transfer of prescriber prescription data from data miners to brand-name pharmaceutical manufacturers).

*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).

*Sorrell*, 630 F.3d at 267 (defining the practice of detailing).

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

*Id.* at 46; Baxter, *supra* note 48, 650 (describing pharmaceutical marketers’ direct-to-physician approach);

*Heesters*, *supra* note 5, 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).


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

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

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

*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).

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

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

*Sorrell*, 630 F.3d at 267-68 (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, 246 (arguing that the most aggressive marketing is reserved for blockbuster brand-name drugs under patent whose profits exceed all other drugs).

*Connors*, *supra* note 7, 247.

*Mills*, 616 F.3d at 16 (describing IMS Health’s data mining revenues for 2005); *Heesters*, *supra* note 5, 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).

*Orentlicher*, *supra* note 5, 76 (highlighting evidence demonstrating that detailing influences prescribing decisions and increases drug sales); *Weiss*, *supra* note 56 at 262 (arguing that doctors prescribe an advertised drug more frequently once they are subject to detailing).

*Orentlicher*, *supra* note 5, 74 (Spring, 2010) (characterizing the scope of detailing in terms of participant size and costs).
Disclosure of Genetic Information by Relatives

mental illness or cancer is disclosed); Schawbel, supra note 5, 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 56, 268-69 (discussing how detailing results in significant overspending by taxpayers and those with insurance).


Baxter, supra note 48, 652 (describing recent prescription drug cost trends).

So rell, 630 F.3d at 293 (Livingston, J., dissenting) (finding that the risks associated with generic drugs are more well known).

Orentlicher, supra note 5, 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).

Connors, supra note 7, 277.

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


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, 76 (addressing the negative impacts when a patient’s drug abuse, STD, mental illness or cancer is disclosed); Schawbel, supra note 3, 911-12 (describing the negative consequences of inadequately protected individual health information); Terry & Francis, supra note 79, 696-97 (citing studies of behaviors patients engage in to protect their privacy, but which can have negative impacts on patient health outcomes).

Adelman & Zahler, supra note 3, 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, 947 (discussing how inadequate privacy protections for prescription PHI will interfere with pharmacists’ ability to perform their patient counseling obligations under OBRA 1990).

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

Id. at 195.

Id. at 205, 213.

Id. at 214-20.

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).


Restatement (Second) of Torts §§ 652B (1977) (intrusion upon seclusion requires demonstrating intentional intrusion upon private affairs that would be highly offensive to a reasonable person).

Adelman & Zahler, supra note 3, 134 (listing the likely common law torts for protecting against improper disclosure of medical information); Terry, supra note 6, 5-6 (distinguishing between tortuous 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, supra note 79, 712-13 (discussing the application of the breach of confidence tort within the context of health information).

90 Poli v. Mountain Valleys Health Centers, Inc., 2006 WL 83378 at *4 (E.D. Cal. 2006) (denying 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., 1999 WL 494114 at *1 (Mass. Super. Ct. 1999) (denying summary judgment on 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’ names, addresses, dates of birth, prescription and medical information to a mailing service, which sent out drug manufacturer funded mailings to patients reminding them to refill certain prescriptions or providing information regarding new drugs); Anonymous v. CVS Corp., 188 Misc.2d 616, 621 (N.Y. Sup. Ct. 2001), aff’d by Anonymous v. CVS Corp., 293 A.D.2d 285 (N.Y. App. Div. 2002) (denying motion to dismiss of breach of confidentiality claim against pharmacy that sold HIV patient’s prescription information to chain drug store without patient’s knowledge or consent). See also Terry, supra note 6, 5 n. 18 (listing state court cases recognizing common law protections for health information).


92 Lawson v. Mecon, 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 statute regarding improper disclosure of patient medical records was no preempted by HIPAA where patient sued provider and provider’s employees under the Minnesota statute 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 pharmacy’s disclosure of wife’s prescription records to attorney for husband without knowledge or consent of wife or court violated Rhode Island’s Confidentiality of Health Care Information Act). See also Terry, supra note 6, 5 n. 19 (listing state statutes providing for the protection of health information).

93 Anonymous, 188 Misc.2d at 621 (denying motion to dismiss of pharmacy that sold HIV patient’s prescription information to chain drug store without patient’s knowledge or consent).

94 Weld, 1999 WL 494114 at *1 (denying summary judgment on 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’ names, addresses, dates of birth, prescription and medical information to a mailing service, which sent out drug manufacturer funded mailings to patients reminding them to refill certain prescriptions or providing information regarding new drugs).

95 Washburn, 695 A.2d at 498-500.

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


100 Vermont v. Welch, 624 A.2d 1105, 1109, 1112 (Vt. 1992)

101 Fanean, 984 A.2d at 821, 824-25.

102 Fanean, 984 A.2d 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).
103 Mowery, supra note 2, 712 (arguing that a patient’s right to privacy is protected on a state level, but the protections vary from state to state).

104 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”).

105 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, 947-48.


110 45 C.F.R. §§ 160.102 and 160.103 (2011). The entities covered by the 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 the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40868-01 (proposed July 14, 2010) (to be codified at 45 C.F.R. § 160.102(b)) (addressing the expansion of HIPAA restrictions to business associates of covered entities).


123 Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40868-01.


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

126 Id. at 38, citing 45 C.F.R. § 164.514(b)(2)(i) (2011).


129 Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information, 74 Fed. Reg. at 19008.


131 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).

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).


Mowery, supra note 2, 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 Amendments guarantee of liberty).

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).

Schawbel, supra note 3, 941 (describing the different aspects of the constitutional right to privacy).

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

Whalen, 429 U.S. at 589, 591 (holding that the state’s police power justified any privacy invasion resulting from the maintenance of a state mandated centralized prescription monitoring system).

Whalen, 429 U.S. at 597-98.

Whalen, 429 U.S. at 600.

Whalen, 429 U.S. at 602.

Whalen, 429 U.S. at 603, n. 30.

Whalen, 429 U.S. at 603-604.

Whalen, 429 U.S. at 605.

Ward, supra note 5, 76 (noting that courts have varied in their holdings as to the level of protection afforded to an individual’s privacy right in prescription data and that the magnitude of the right has not been completely defined); Woodage, supra note 87, 688 (noting a Circuit split with regard to whether or not the Constitution protects against the disclosure of personal information).


Woodage, supra note 87, 688, citing Doe v. Wigginton, 21 F.3d 733, 740 (6th Cir. 1994).

Woodage, supra note 87, 688, citing Alexander v. Peffer, 993 F.2d 1348, 1350 (8th Cir. 1993).

Doe v. Southeastern Pennsylvania 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).

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).

Id. at 1143 (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”).

Id. at 1139-40, 1143.

Douglas v. Dobbs, 419 F.3d 1097, 1102 (10th Cir. 2005) (holding that Assistant District Attorney in civil rights action was entitled to qualified immunity for approving law enforcement request to search patient’s pharmacy records for evidence of abuse of pain medication).

Id. at 1102, n. 3.

United States v. Sutherland, 143 F. Supp.2d 609, 610 (W.D. Va. 2001) (holding that hospital could not produce patients’ pharmacy records at trial without giving patients an opportunity to object).

Id. at 611-12; Ward, supra note 5, 76 (noting that courts have held that a patient’s interest in privacy must be balanced against the state’s ability to exercise its police power and protect public welfare).

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

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

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).
N.H. Rev. Stat. Ann § 318:47-f (2011). See also N.H. Rev. Stat. Ann § 318-B12(IV) (2011) (providing that “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 required 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.”)


Mills, 616 F.3d at 13 (upholding the constitutionality of the Maine data mining statute on the grounds that the statute regulated conduct and not speech).

Id.

Id. at 19.

Id. at 21.

Id. at 22.

Id.

Id. at 14.

Id. at 26, 28.

Id. at 32.

Id.

Id.

Id. at 36 (Lipez, J., concurring).

Sorrell, 630 F.3d at 266-67 (holding that the Vermont statute 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).

Id. at 272.

Id.

Id. at 273.

Id. at 274.

Id. at 275.

Id. at 275-76.

Id. at 276.

Id.

Id. at 277.

Id.

Id. at 277-78.

Id. at 279.

Id.

Id. at 281.

Id.

Id. at 276

Id. at 290 (Livingston, J., dissenting).

Id. at 291 (Livingston, J., dissenting).

Id. at 293-97 (Livingston, J., dissenting).


Mills, 616 F.3d at 33 (Lipez, J., concurring) (noting that the Maine statute does not actually directly limit drug companies or detailers’ marketing efforts using prescriber-identifiable information).


Vt. Stat. Ann. Tit. 18, § 4631(d); Mills, 616 F.3d at 33, n. 37 (Lipez, J., concurring) (noting that the Vermont statute “also bars pharmaceutical manufacturers and marketers from using the information for marketing or promoting a prescription drug unless the prescriber consents”).


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).

Id. at 41(Lipez, J., concurring).


Sorrell, 630 F.3d at 270 (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); Ayotte, 550 F.3d at 61 (finding the intent of the New Hampshire law to be the prevention of targeted detailing by pharmaceutical companies using prescriber histories).


Sorrell, 630 F.3d at 283 (Livingston, J., dissenting) (noting that detailers are prohibited from directly referencing prescriber information data in their detailing visits by the terms of the pharmaceutical manufacturers’ licensing agreements with the data miners).


Mills, supra note 48, 653 (outlining the PDRP program).

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


Weiss, supra note 56, 274 (arguing that the PhRMA Code’s voluntary compliance provision invites noncompliance). Notably, the PhRMA Code only applies to the pharmaceutical companies, whereas the data-collection industry is completely unregulated. Mowery, supra note 2, 701.

Connors, supra note 7, 278.


Mowrey, supra note 2, 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, 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”).

Mowrey, supra note 2, 718; Schawbel, supra note 3, 958.

Schawbel, supra, note 3, 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).

Ayotte, 550 F.3d at 103 (Lipez, J., concurring and dissenting) (recounting that data miners’ transactions regarding prescription data take place out-of-state).

Schawbel, supra note 3, 956 (arguing that the protection of pharmacist-patient confidentiality is weak, if the pharmacist’s employer does not respect it).

Han, supra note 2, at 135 (arguing for the need for the need for more comprehensive federal regulation to protect the privacy of patient PHI); Schawbel, supra note 3, 925 (arguing that privacy protection of medical records is hindered by the lack of uniformity among state laws); Terry & Francis, supra note 79, 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).

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


Terry, supra note 6, 4 (contending that the common law right to privacy “promises far more than it delivers”).

Terry & Francis, supra note 79, 711-12 (arguing that common law privacy torts provide inadequate protection for the privacy of health data).
266 Id. at 712. See also Terry, supra note 6, 4-5 (citing Knight v. Penobscot Bay Med. Ctr., 420 A.2d 915 (Me. 1980), Estate of Berthiaume v. Pratt, 365 A.2d 792 (Me. 1976), and Swarthout v. Mutual Serv. Life Ins., 632 N.W.2d 741 (Minn. Ct. App. 2001) as illustrative of the difficulties in applying common law privacy torts to the field of healthcare).
267 Mowery, supra note 2, 714.
268 Id. at 714-15 (noting that “no state expressly provides for a pharmacist-patient privilege”).
269 DeVries, supra note 30, 288 (2003) (arguing that common law torts provide inadequate protection for informational privacy).
270 Id. at 307.
271 Mowery, supra note 2, 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).
272 Terry & Francis, supra note 79, 713 (discussing the weaknesses of state privacy and confidentiality statutes with regard to protecting the privacy of health information).
273 DeVries, supra note 30, 289 (arguing that state and federal statutes designed to protect informational privacy are insufficient to achieve that goal).
275 DeVries, supra note 30, 288-89 (criticizing state constitutional privacy protections as inadequately protecting informational privacy).
276 Glenn, supra note 91, 1612 (noting that constitutional privacy protections lack the capacity to protect against invasions of privacy by private actors); Schawbel, supra note 3, 952 (noting that legislation protecting the privacy of prescription records within the private sector is lacking).
277 Edmonson v. Leesville Concrete Co., Inc., 500 U.S. 614, 619 (1991) (holding that “the Constitution’s protections of individual liberty and equal protection apply in general only to action by the government”).
279 Id.
280 Whalen, 429 U.S. at 605 (holding that the right to privacy in personal information is not absolute in the context of “the 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, 288 (contending that federal courts are overly deferential to government justifications for collecting private personal information).
281 Burton’s Pharmacy, Inc. at ¶1; The Muecke Company, Inc. at ¶14-17;
282 Schawbel, supra note 3, 942 (discussing why the constitutional right to privacy does not adequately protect the right to privacy in health information).
283 DeVries, supra note 30, 288 (arguing that constitutionally protected privacy interest in “‘avoiding disclosure of personal matters’ does not seem very broad”).
284 Id.
285 Terry, supra note 6, 31 (criticizing the HIPAA standards as lacking transparency and clarity); Terry & Francis, supra note 79, 715 (arguing that the partial preemption by HIPAA of state privacy protections creates confusion and renders HIPAA operationally obstructive).
286 45 C.F.R. § 160.102(a) (2011); Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40868-01 (to be codified at 45 C.F.R. 160.102(b)) (addressing the expansion of HIPAA restrictions to business associates of covered entities); Terry & Francis, supra note 79, 716 (criticizing HIPAA for its failure to apply privacy protections to all medical data and all users of such data).
287 Hilary M. Wandall, An Overview of Privacy Laws Impacting Pharmaceutical Companies, 878 PLI/Pat 509, 516 (October, 2006) (describing the limitations of HIPAA in terms of covered entities, particularly within the pharmaceutical industry).
288 Terry, supra note 6, 31; Terry & Francis, supra note 79, 683-84 (describing HIPAA’s privacy protections as sieve-like).
289 Terry, supra note 6, 717 (arguing that HIPAA’s regulations read like a catalogue of exceptions to confidentiality and/or set of “process rules for authorizations to avoid confidentiality”).
290 Burton’s Pharmacy, Inc. at ¶32 (describing CVS Caremark’s alleged justification for sharing patient prescription PHI with the Caremark side of CVS Caremark).
70

292 Burton’s Pharmacy, Inc. at ¶32.
293 Terry & Francis, supra note 79, 715-16; Wandall, supra note 287, 517 (noting that the HIPAA Privacy Rule “permits disclosure of product safety data to pharmaceutical manufacturers . . . without an authorization”).
294 Terry & Francis, supra note 79, 714-15 (outlining the flaws and limitations of HIPAA).
296 Terry, supra note 6, 3 (arguing that the United States legal system is “only dimly cognizant of the de-identification model”).
297 Gellman, supra note 16, 37-38 (noting that HIPAA’s Privacy Rule assumes that data de-identified according to the Privacy Rule standards provides complete anonymity, when it actually carries a risk of re-identification, particularly when public records are consulted for re-identification purposes).
298 45 C.F.R. § 14.50(d)(1) (2011) (requiring removal of 18 specific identifiers for data to be considered de-identified under HIPAA).
299 Klocke, supra note 6, 511-12 (illustrating what HIPAA de-identified health records might look like).
300 Sorrell, 630 F.3d at 283, n. 4; Ayotte, 550 F.3d at 45.
302 45 CFR § 164.312(a)(2)(iv) and (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. at 40916-17 (to be codified at 45 CFR §§164.106 and 164.306) (proposing to directly subject business associates to the Security Rule standards).
303 Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009, 74 Fed. Reg. at 19009.
305 Terry, supra note 6, 257.
306 Id. at 251 (noting that HHS’ Office of Civil Rights has control over HIPAA enforcement, not patients); Terry & Francis, supra note 79, 713.
307 Terry, supra note 6, 7-8, 13 (describing HIPAA’s enforcement mechanism). See 45 C.F.R. § 164.530 (2011).
308 Terry, supra note 6, 13.
309 Terry, supra note 6, 236 (citing evidence that medical data is still at risk under HIPAA).
310 Id. at 239.
311 Gellman, supra note 16, 34 (arguing that “no 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 re-identified”).
312 Elizabeth Hutton & Devin Barry, Privacy Year in Review: Developments in HIPAA, 1 I/S: J. L. & Pol’y for Info. Soc’y 347, 379 (2005) (arguing that additional federal legislation is needed to uniformly protect patient privacy because HIPAA fails to preempt state law); Mowery, supra note 2, 738 (contending that “the likelihood of every state enacting model or uniform laws is very small”).
313 Burton’s Pharmacy, Inc. at ¶¶ 62-69; The Muecke Company, Inc. at ¶¶ 123-34; Mowery, supra note 2, 735 (arguing that federal legislation “would be able to standardize the management of patient information).
314 Hutton & Barry, supra note 312, 379.
315 Mowery, supra note 2, 718-19 (noting that varying state privacy laws create problems for patients who move from one state to another).
316 Id. (noting that varying state privacy laws create problems for patients who receive treatment in different states).
317 Klocke, supra note 6, 535 (arguing that “state-by-state regulation may slow interstate commerce as large retail chain pharmacies and other covered entities who business crosses state borders would have to customize [prescription] data to meet the requirements of each individual state before the data are transferred”).
318 Mowery, supra note 2, 739.
319 Id.
320 DeVries, supra note 30, 291.
321 Id.
access); Terry & Francis, to confirm the identity of anyone using the [electronic medical record] system and to guarantee against unauthorized
Hiller, are mandatory penalties for violations due to willful neglect, which may lead to strengthened enforcement. Janine
enforcement action by regulators over HIPAA”). With the passage of HITECH, penalties are increased and there
N. Ill. U. L. Rev. 531, 551-52 (2010) (describing a “major uproar by privacy advocates has emerged over the lack of
information cannot be kept confidential).
automatically amount to an impermissible invasion of privacy”).
disclosures to representatives of the State having responsibility for the health of the community, does not
practice even when the disclosure may reflect unfavorably on the character of the patient. Requiring such
personnel, to insurance companies, and to public health agencies are often an essential part of modern medical
health care providers).
information); Terry, supra note 3, 951-52 (discussing the advantages and disadvantages of complete preemption for federal
legislation protecting medical record privacy).
Sorrell supra note 6, 714-15 (arguing that HIPAA’s principal achievement was to require notice of privacy
practices to be given to patients by covered entities and that HIPAA lacks a consent-to-disclosure requirement for most healthcare activities).
See generally Burton’s Pharmacy, Inc.; The Muecke Company, Inc.
Rosoff, supra note 2, 26 (contending that people want to be able to control who has access to their medical
information); Terry, supra note 6, 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).
Terry & Francis, supra note 79, 701-03 (describing various options for protecting patient privacy in electronic health record systems, including allowing patients to specify that records from certain providers, records from certain or certain types of information from their medical records be kept out of electronic health record systems).
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 silo-ed).
Burton’s Pharmacy, Inc. at §32.
Whalen, 429 U.S. at 602 (holding that “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. Requiring such disclosures to representatives of the State having responsibility for the health of the community, does not automatically amount to an impermissible invasion of privacy”).
Id.
Terry & Francis, supra note 79, 704 (describing public health and law enforcement scenarios in which health
information cannot be kept confidential).
Mills, 616 F.3d at 40-41 (Lopez, J., concurring).
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 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
Terry, supra note 6, 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”); Terry & Francis, supra note 79, 704-06 (proposing the need for and importance of a tracking system
within the context of electronic health records and advocating for patient notification of unauthorized disclosures).
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 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, 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).
Reid Skibell, Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act, 18
Berkeley Tech. L.J. 909, 938 (2003) (contending that “it is generally accepted that the threat of being hacked has led to a revolution in computer security”).
Gellman, supra note 16, 34 (arguing that “encryption, or other mathematical approaches to de-identification aimed at protecting privacy fail to provide solutions to address all data types and data sharing activities”).
Terry & Francis, supra note 79, 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).
Mowery, supra note 2, 736 (discussing the use of audits to determine who has used patient information and for determining whether such access was fraudulent).
Weiss, supra note 56, 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).

Central Hudson Gas & Elec. Corp., 447 U.S. at 564 (holding that restrictions on commercial speech must be justified by a substantial state interest).

Whalen, 429 U.S. at 603-604; Douglas, 419 F.3d at 1102; SEPTA, 72 F.3d at 1139-40.

Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 883-84 (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, 518 (arguing that a lapse in physician privacy is “a derivative of a lapse in patient privacy”).

Central Hudson Gas & Elec. Corp., 447 U.S. at 564 (holding that restrictions on commercial speech must be narrowly tailored to directly promote a substantial state interest).


Mills, 616 F.3d at 15 (describing prescribers’ objections to detailing as intruding into their prescribing decisions).

Id. at 22 (holding that “targeted prohibitions are by definition less restrictive [of speech] than a categorical ban”).


Cicconi, supra note 351, 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 Freedom of Religion 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 right to object to providing birth control medication to a patient, for religious reasons, in direct conflict with a woman’s constitutional right to privacy”).

Contrast 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 unconstitutional 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); 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); Kubasek, et al., supra note 352, 261 (arguing that “the constitutional right to privacy and potential obstacles to obtaining birth control outweigh pharmacists’ interest in exercising their religion”); 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 351, 557 (arguing that ultimately the pharmacist’s right to freedom 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); Jason R. Mau, Stormans and the Pharmacists: Where have all the Conscience 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).

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 603-604; Douglas, 419 F.3d at 1102; SEPTA, 72 F.3d at 1139-40 (collectively recognizing that there is no absolute right to privacy in prescription information).

Whalen, 429 U.S. 602-03 (allowing restriction on right to privacy in patient prescription information for purposes of monitoring illegal drug diversion).

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

Klocke, supra note 6, 531.
Orentlicher, supra note 5, 81 (drawing an analogy to the lower scrutiny applied to a commercial speech restriction where the government is funding the speech of private citizens).

Id. at 81.

Weiss, supra note 56, 285 (arguing that medical marketing regulations should pass First Amendment commercial speech intermediate scrutiny as long as such regulations do not prohibit pharmaceutical manufacturers from communicating truthful marketing or educational information to physicians).

Id. at 291 (arguing that pharmaceutical manufacturers’ profit motive would likely diminish any chilling effect attendant to a marketing regulation); Klocke, supra note 6, 533-34 (noting that the Supreme court has pointed out that “commercial speech is hardy and unlikely to be deterred by regulation”).