


September 2014

Minding Your Meds: Balancing the Needs for Patient Privacy and Law Enforcement in Prescription Drug Monitoring Programs

Devon T. Unger
West Virginia University School of Law

Follow this and additional works at: <https://researchrepository.wvu.edu/wvlr>

 Part of the [Constitutional Law Commons](#), [Fourth Amendment Commons](#), [Law Enforcement and Corrections Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Devon T. Unger, *Minding Your Meds: Balancing the Needs for Patient Privacy and Law Enforcement in Prescription Drug Monitoring Programs*, 117 W. Va. L. Rev. (2014).

Available at: <https://researchrepository.wvu.edu/wvlr/vol117/iss1/11>

This Student Note is brought to you for free and open access by the WVU College of Law at The Research Repository @ WVU. It has been accepted for inclusion in West Virginia Law Review by an authorized editor of The Research Repository @ WVU. For more information, please contact ian.harmon@mail.wvu.edu.

**MINDING YOUR MEDS:
BALANCING THE NEEDS FOR PATIENT PRIVACY AND LAW
ENFORCEMENT IN PRESCRIPTION DRUG MONITORING
PROGRAMS**

I.	INTRODUCTION.....	346
II.	A BRIEF OUTLINE OF STATE PDMPs.....	348
	<i>A. A Brief History of State PDMPs and Common Variations Among the Programs</i>	349
	<i>B. Studies of PDMP Effectiveness</i>	350
	<i>C. Criticism of and Litigation Involving PDMPs</i>	352
III.	THE APPLICABLE LAW: THE FOURTH AMENDMENT, HEALTHCARE- SPECIFIC PRIVACY LAWS, AND THE ADMINISTRATIVE SUBPOENA	354
	<i>A. The Fourth Amendment Generally</i>	354
	<i>B. The Fourth Amendment and Medical Information</i>	357
	<i>C. Other Sources of Privacy Protection for Health Information</i>	362
	<i>D. The Administrative Subpoena</i>	364
IV.	A PATIENT’S LEGITIMATE EXPECTATION OF PRIVACY IN PDMP DATA JUSTIFIES A WARRANT REQUIREMENT.....	368
	<i>A. Patients Have a Legitimate Expectation of Privacy in Their PDMP Data</i>	368
	1. Patients Have a Subjective Expectation of Privacy in Their PDMP Data	369
	2. Society Is Prepared To Recognize this Expectation as Objectively Reasonable.....	369
	3. Privacy Expectations for Health Information, Including PDMP Data, Have Sources Beyond the Fourth Amendment...	371
	<i>B. Law Enforcement Must Show Probable Cause and Obtain a Warrant Before Accessing PDMP Data</i>	373
	1. The State’s Interest in Law Enforcement Does Not Outweigh a Patient’s Legitimate Expectation of Privacy in Their PDMP Data	373
	2. Administrative Subpoenas Cannot Be Used To Obtain PDMP Data	375
	3. State PDMPs That Allow Law Enforcement To Access the Data Without a Warrant Are Unconstitutional.....	378
	<i>C. States Should Include Privacy Protection Within Their PDMPs</i> ...	378

V.	BALANCING THE INTERESTS OF EVERYONE: HOW TO GIVE LAW ENFORCEMENT ACCESS TO PDMP DATA WITHOUT VIOLATING PATIENT PRIVACY	380
VI.	CONCLUSION	382

I. INTRODUCTION

One evening in July 2009, 26-year-old Nick Bills parked his pickup truck outside a bar in St. Marys, West Virginia.¹ He extracted the synthetic prescription painkiller fentanyl from a patch designed to slowly release the medicine through the skin, mixed it with water, and injected the drug directly into his veins.² Bills began using prescription pain medicine after undergoing surgery for a shattered elbow.³ Doctors prescribed him so many pills, the bottles “covered the top of the refrigerator”⁴ At first he gave extra pills away to friends, but after a while, his own addiction took hold.⁵ Eventually, popping pills became shooting up fentanyl in a parking lot.⁶ Nick Bills died in that parking lot on July 19, 2009, and he, as well as thousands of others over the last decade, are tragic examples of the consequences that accompany a rise in prescription drug abuse.⁷

From 1992 to 2008, prescription drug overdose deaths in the United States have more than tripled.⁸ For more than a decade, deaths from drug abuse have surpassed homicide, suicide, and gunshot wounds as causes of death; this upsurge was attributed largely to the increased abuse of prescription drugs.⁹ The increase in prescription drug abuse has had a particularly devastating impact in Appalachia, exemplified by West Virginia, which led the nation in

¹ Alison Knezevich, *Prescription Drug Abuse Takes Deadly Toll in W. Va.*, CHARLESTON GAZETTE, Jan. 15, 2011, <http://www.wvgazette.com/News/201101151175>.

² *Id.*; *Fentanyl Transdermal Patch*, NAT’L INST. OF HEALTH, <http://www.nlm.nih.gov/medlineplus/druginfo/meds/a601202.html#how> (last visited Oct. 15, 2014).

³ Knezevich, *supra* note 1.

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*; Miles D. Schreiner, *A Deadly Combination: The Legal Response to America’s Prescription Drug Epidemic*, 33 J. LEGAL MED. 529, 530–31 (2012).

⁸ CTRS. FOR DISEASE CONTROL, POLICY IMPACT: PRESCRIPTION PAINKILLER OVERDOSES 3–4 (2011) [hereinafter POLICY IMPACT], available at <http://www.cdc.gov/homeandcreational/safety/pdf/policyimpact-prescriptionpainkillerod.pdf>. Prescription painkiller overdose deaths rose from less than 4,000 in 1990 to 14,800 in 2008. *Id.*

⁹ Schreiner, *supra* note 7, at 530–31.

overdose deaths per capita in 2010.¹⁰ West Virginia's overdose death rate rose from 6.2 per 100,000 residents in 2000, to 28.9 per 100,000 in 2010.¹¹ West Virginia was one of 29 states where drug overdose deaths exceeded auto accident deaths, highlighting the nationwide impact of the rise in prescription drug abuse.¹² Multiple factors have fueled the increase in abuse, including a growing acceptance of opioids, such as oxycodone and hydrocodone, to treat pain and the resulting increase in doctors' willingness to prescribe the drugs, sometimes to excessive levels; "doctor shopping" by patients; and improper prescriptions by physicians, sometimes through clinics dubbed "pill mills"¹³ due to the prescribing practices.¹⁴

The states and the federal government responded to this rise in prescription drug abuse with widespread implementation of state prescription drug monitoring programs ("PDMPs")¹⁵ and federal monitoring legislation signed into law in 2005.¹⁶ PDMPs are electronic databases that collect and store information regarding prescription drugs and patients, including patients' names, addresses, drug histories, prescribers, and dispensers.¹⁷ Health care providers and law enforcement have used these programs to combat the rise in

¹⁰ Reid Wilson, *Drug Overdoses Kill More People than Auto Accidents in 29 States*, WASH. POST, Oct. 8, 2013, <http://www.washingtonpost.com/blogs/govbeat/wp/2013/10/08/drug-overdoses-kill-more-people-than-auto-accidents-in-29-states/>.

¹¹ *Id.*

¹² *Id.*

¹³ See *Abuse of Controlled Prescribed Substances Continues to be Nation's Fastest-Growing Drug Problem*, CONTROLLED SUBSTANCES HANDBOOK NEWSL., Jan. 2014, at 2 (providing a concise description of characteristic pill mill practices).

¹⁴ Laxmaiah Manchikanti, *Prescription Drug Abuse: What Is Being Done to Address This New Drug Epidemic? Testimony Before the Subcommittee on Criminal Justice, Drug Policy and Human Resources*, 9 PAIN PHYSICIAN 287, 299-300 (2006); Barry Meier, *A New Painkiller Crackdown Targets Drug Distributors*, N.Y. TIMES, Oct. 17, 2012, <http://www.nytimes.com/2012/10/18/business/to-fight-prescription-painkiller-abuse-dea-targets-distributors.html?pagewanted=all> [hereinafter Meier, *Painkiller Crackdown*]; Barry Meier, *Tightening the Lid on Pain Prescriptions*, N.Y. TIMES, Apr. 8, 2012, <http://www.nytimes.com/2012/04/09/health/opioid-painkiller-prescriptions-pose-danger-without-oversight.html?pagewanted=all>.

¹⁵ See KAREN BLUMENSCHIN ET AL., KENTUCKY ALL SCHEDULE PRESCRIPTION ELECTRONIC REPORTING PROGRAM (KASPER) EVALUATION TEAM, REVIEW OF PRESCRIPTION DRUG MONITORING PROGRAMS IN THE UNITED STATES (2010), available at <http://chfs.ky.gov/NR/rdonlyres/85989824-1030-4aa6-91e1-7f9e3ef68827/0/Kasperevaluationpdmstatusfinalreport6242010.pdf>.

¹⁶ Gloria Goodale, *Prescription Drug Abuse Surged 400 Percent in Past Decade*, CHRISTIAN SCI. MONITOR, July 15, 2010, available at <http://www.csmonitor.com/USA/2010/0715/Prescription-drug-abuse-surged-400-percent-in-past-decade>.

¹⁷ *E.g.*, FLA. STAT. § 893.055(3) (2014); OR. REV. STAT. § 431.964 (2013); W. VA. CODE § 60A-9-4(a)(1)-(9) (2014).

drug abuse, but the programs have raised Fourth Amendment privacy concerns for patients relating to the access and use of PDMP information.¹⁸

This Note argues that patients have a legitimate expectation of privacy in their personally identifiable PDMP data, and the Fourth Amendment requires that law enforcement obtain a warrant before accessing personally identifiable PDMP data. In addition, it also advocates for the utilization of other means to protect patient privacy, such as exempting PDMP data from public records laws, and imposing civil and/or criminal penalties for the wrongful access, use, and dissemination of PDMP data. Lastly, the Note proposes a solution that gives law enforcement warrantless access to de-identified PDMP data so as to balance the need to enforce drug laws with patients' expectation of privacy.

Part II of this Note provides background information, including an outline of PDMPs, how they started, how they operate, and an examination of studies relating to their effectiveness. Part III also provides background by discussing the law relevant to this Note's analysis, including Fourth Amendment precedent, extra-constitutional privacy laws, and the administrative subpoena power. Part IV applies the law to PDMP data, demonstrating through its analysis that patients have a legitimate expectation of privacy in their personally identifiable PDMP data, and the Fourth Amendment requires that law enforcement obtain a warrant before accessing personally identifiable PDMP data. Finally, Part V proposes measures that could help to effectively balance the patients' privacy interests with the government's interest in enforcing controlled substance laws.

II. A BRIEF OUTLINE OF STATE PDMPs

In order to help the reader understand the importance of this Note's later privacy analysis relating to PDMPs, this Part describes what PDMPs are, how they operate, and privacy concerns they may raise. Section A of this Part discusses the history of state PDMPs, and some of the varied particularities of the programs. Section B examines some studies conducted by individual states that have measured the effectiveness of their programs, as well as some potential issues that these programs create. Finally, Section C of this Part discusses criticism and litigation that has arisen as PDMPs have been utilized for the purpose of obtaining evidence for criminal prosecutions.

¹⁸ Christian Gaston, *Oregon Sues DEA Over Access to Patient Drug Records*, OREGONLIVE (Nov. 30, 2012), http://www.oregonlive.com/politics/index.ssf/2012/11/oregon_sues_dea_over_access_to.html.

A. *A Brief History of State PDMPs and Common Variations Among the Programs*

Between 1939—when California created the first PDMP—and 1992, ten states¹⁹ passed laws creating PDMPs.²⁰ In the 22 years since, 39 other states and the District of Columbia enacted legislation to create PDMPs.²¹ Although the federal monitoring program, the National All Schedule Prescription Electronic Reporting Act (“NASPER”), was passed and signed into law in 2005, it has yet to be funded.²² If fully funded and implemented, NASPER would establish PDMPs in all 50 states and allow doctors to access databases in neighboring states.²³ NASPER received \$2 million per year in appropriations in 2009 and 2010, which it used to fund grants to help states implement and operate their programs.²⁴

PDMPs generally serve multiple specific purposes,²⁵ generally aimed at reducing prescription drug abuse, while ensuring access for those with legitimate medical needs.²⁶ This Note specifically addresses privacy issues relating to the purpose of PDMPs as a “tool that serves the needs of [law enforcement].”²⁷ These monitoring programs vary from state to state in terms of the drugs they monitor, how they collect and distribute the information, who

¹⁹ The first ten states to pass PDMPs between 1939 and 1992 were California (1939), Hawaii (1943), Illinois (1958), Idaho (1967), Pennsylvania (1972), New York (1972), Rhode Island (1978), Texas (1982), Michigan (1988), and Oklahoma (1990). BLUMENSCHNEIN ET AL., *supra* note 15, at 6–7.

²⁰ *Id.* at 2.

²¹ NAT’L ALLIANCE FOR MODEL STATE DRUG LAWS, PRESCRIPTION DRUG ABUSE, ADDICTION AND DIVERSION: OVERVIEW OF STATE LEGISLATIVE AND POLICY INITIATIVES, PART 1: STATE PRESCRIPTION DRUG MONITORING PROGRAMS (PMPS) 6 (2014) [hereinafter NAMSDDL], available at <http://www.namsdl.org/library/884CB2C5-1372-636C-DD54DCC00FD31313/>.

²² Richard M. Reisman et al., *Prescription Opioid Usage and Abuse Relationships: An Evaluation of State Prescription Drug Monitoring Program Efficacy*, 3 SUBSTANCE ABUSE: RES. & TREATMENT 41, 50 (2009).

²³ *Id.*

²⁴ KRISTIN M. FINKLEA ET AL., CONG. RES. SERV., R42593, PRESCRIPTION DRUG MONITORING PROGRAMS 16 (2013), available at <http://www.hsdl.org/?view&did=728239>.

²⁵ These purposes include:

- (1) to support access to legitimate medical use of controlled substances, (2) to help identify and deter or prevent drug abuse and diversion, (3) to facilitate and encourage the identification, intervention with, and treatment of persons addicted to prescription controlled substances, (4) to help inform public health initiatives through outlining of use and abuse trends, and (5) to help educate individuals about PMPs and prescription drug use, abuse, diversion, and addiction.

NAMSDDL, *supra* note 21, at 11.

²⁶ *Id.*

²⁷ *Id.*

has access to the information, the agency responsible for administering the program, how the program is funded, who is required to report information, and whether participation is mandatory.²⁸

All programs monitor at least Schedule II drugs,²⁹ most monitor drugs in Schedules II–IV, and 17 monitor non-scheduled or non-controlled drugs.³⁰ Almost all programs authorize both prescribers (doctors) and dispensers (pharmacists) to use and access the information.³¹ Almost all programs also authorize law enforcement to use the program to obtain evidence in criminal investigations, but states vary with regard to the scope of access afforded to law enforcement.³² Some states, such as Oregon, require law enforcement to have a search warrant or a showing of probable cause before gaining access to information from the program.³³ Others require that the request for information be pursuant to an active investigation.³⁴ Pennsylvania, which houses its program within the Office of the Attorney General, requires law enforcement to obtain approval from the attorney general to obtain information from the program.³⁵ A few states have conducted evaluations of their programs, with mixed results.³⁶

B. *Studies of PDMP Effectiveness*

Some models that evaluate the effects of PDMPs have indicated that the programs generally reduce the supply of Schedule II pain relievers and stimulants.³⁷ Maine found its program to be effective for identifying patients that were doctor shopping, recognizing and treating individuals addicted to prescription drugs, and protecting patient confidentiality.³⁸ Maine's evaluation

²⁸ *Id.*

²⁹ The Federal Drug Enforcement Administration organizes controlled substances into five schedules, I–V. Schedule I contains illegal drugs with no legitimate medical purpose, Schedule II contains the most dangerous and addictive drugs that may be prescribed for legitimate medical purposes, and the drugs in the remaining schedules decrease in their danger, abuse potential, and addiction potential from Schedule III–V. *Drug Scheduling*, DEA, <http://www.justice.gov/dea/druginfo/ds.shtml> (last visited Oct. 15, 2014).

³⁰ NAMSDDL, *supra* note 21, at 13; BLUMENSCHNEIN ET AL., *supra* note 15, at 6–7.

³¹ NAMSDDL, *supra* note 21, at 25.

³² *Id.* at 29.

³³ *Id.*

³⁴ *Id.*

³⁵ *Id.*

³⁶ BLUMENSCHNEIN ET AL., *supra* note 15, at 20–23.

³⁷ RONALD SIMEONE & LYNN HOLLAND, SIMEONE ASSOCIATES INC., AN EVALUATION OF PRESCRIPTION DRUG MONITORING PROGRAMS 19–20 (2006), available at <http://www.simeoneassociates.com/simeone3.pdf>.

³⁸ BLUMENSCHNEIN ET AL., *supra* note 15, at 20–21.

also indicated that the program did not produce a chilling effect on the number of prescriptions doctors were writing.³⁹

However, a study in Virginia found that its program was producing a chilling effect for Schedule II prescriptions.⁴⁰ Virginia's study also demonstrated a low utilization rate of the program by prescribers, dispensers, and other authorized users; regardless, 68% of physicians still said the program "is useful for monitoring their patients' prescription history and decreasing the incidence of 'doctor shopping.'"⁴¹ Finally, an evaluation of Kentucky's PDMP found a high, and likely increasing, utilization of the program; no chilling effect on prescriptions; and that the program was effective at helping to identify abuse and gathering information during criminal investigations.⁴²

Multiple organizations have produced best practice guidelines for PDMPs or model PDMP laws.⁴³ These groups generally agree on what the best practices for PDMPs consist of, including mandatory reporting and use; distribution of proactive alerts regarding suspicious activity; interstate sharing of data; and penalties for unlawful access, use, and disclosure.⁴⁴ However, these groups' views differ somewhat regarding what drugs should be monitored; how states should evaluate their PDMPs; and whether all aspects such as enrollment, reporting, and utilization should be mandatory.⁴⁵

The generally recognized efficacy of the programs has led to many commenters arguing that these programs should be expanded and enhanced to decrease diversion, abuse, and the overall number of drugs prescribed.⁴⁶ The programs can help reduce prescription drug abuse at the front end, by informing doctors' prescribing decisions based on their patients' prescription histories.⁴⁷ Despite the benefits, PDMPs have raised some concerns.

³⁹ *Id.* at 21.

⁴⁰ *Id.* at 21–22.

⁴¹ *Id.*

⁴² *Id.* at 22–23.

⁴³ NAMSDL, *supra* note 21, at 12–13.

⁴⁴ *Id.* at 11–13.

⁴⁵ *Id.* at 13–17.

⁴⁶ See, e.g., Hallam Gugelmann & Jeanmarie Perrone, *Can Prescription Drug Monitoring Programs Help Limit Opioid Abuse?*, 306 J. AM. MED. ASS'N 2258, 2259 (2011) ("Physician, patient, and policy maker advocacy is needed at the state and national level to enhance and expand these monitoring programs."); Christopher M. Jones et al., *Pharmaceutical Overdose Deaths, United States, 2010*, 309 J. AM. MED. ASS'N 657, 659 (2013) ("Tools such as prescription drug monitoring programs . . . can help clinicians to identify risky medication use and inform treatment decisions, especially for opioids and benzodiazepines."); Reisman et al., *supra* note 22, at 50 ("This study supports the efficacy of PDMPs and provides statistical support for establishing PDMPs in all states.").

⁴⁷ See Gugelmann & Perrone, *supra* note 46.

C. Criticism of and Litigation Involving PDMPs

The wave of legislation creating PDMPs has not been without its criticisms. In Florida, one of the last states to pass PDMP legislation,⁴⁸ critics of the program cite concerns over patient privacy, cost, and potential loopholes in the legislation.⁴⁹ Privacy concerns center around the vulnerability of PDMPs as electronic databases, which are susceptible to cyber criminals⁵⁰ and unfettered access by law enforcement agencies.⁵¹

These concerns have been reinforced by litigation in Florida arising out of the disclosure of prescription information by law enforcement to defense counsel during discovery following a sting operation.⁵² A Daytona Beach defense attorney named Michael Lambert sued the state over a disclosure of his personal PDMP data. Lambert brought the suit against Florida State Attorney C.J. Larizza after Lambert's name appeared on a list of 3,300 individuals whose drug histories, doses, pharmacies, and home addresses were provided to five defense attorneys.⁵³ The defense attorneys represented criminal defendants implicated following the sting operation, which targeted a prescription drug trafficking ring.⁵⁴ Lambert contends that a large majority of the names on the list did not need to be disclosed, and the state should have redacted all the names other than those of the six accused individuals.⁵⁵ Lambert's case drew

⁴⁸ See Ashley Dutko, Note, *Florida's Fight Against Prescription Drug Abuse: Prescription Drug Monitoring Program*, 34 NOVA L. REV. 739, 754–58 (2010); Arian Campo-Flores, *Fight Over a Fix for Florida's 'Pill Mills,'* WALL ST. J., Feb. 19, 2011, <http://online.wsj.com/news/articles/SB10001424052748703961104576148753447131080>; Janet Zink & Richard Martin, *Gov. Rick Scott Wants to Repeal Florida's Prescription Drug Monitoring Program*, TAMPA BAY TIMES, Feb. 8, 2011, <http://www.tampabay.com/news/health/gov-rick-scott-wants-to-repeal-floridas-prescription-drug-monitoring/1150411>.

⁴⁹ Dutko, *supra* note 48, at 754–58; Zink & Martin, *supra* note 48.

⁵⁰ See NAMSDL, *supra* note 21, at 15.

⁵¹ Dara Kam, *Critics Skeptical of Official Moves to Safeguard Florida Prescription Database*, PALM BEACH POST, June 19, 2013, <http://www.palmbeachpost.com/news/news/crime-law/critics-skeptical-of-official-moves-to-safeguard-p/nYP8x/>.

⁵² *Id.*

⁵³ *Id.*

⁵⁴ *Id.* The investigation determined that the ring was using false and stolen identities to obtain prescription drugs. *Id.*

⁵⁵ *Id.* The six accused individuals were initially suspected of committing forgery when the records were requested. Following the disclosure and verification by doctors, the investigation found that 63 of the 3,300 names were false, and seven others belonged to victims of identity theft. *Id.*

the attention of the American Civil Liberties Union (“ACLU”),⁵⁶ which also litigated a case in Oregon relating to the use of information from a PDMP.⁵⁷

The case in Oregon involved a conflict between state and federal law.⁵⁸ Oregon law requires law enforcement to obtain a search warrant, with a showing of probable cause, to access information from the state’s PDMP.⁵⁹ Federal law allows certain deputies of the Attorney General to issue administrative subpoenas for information “relevant or material” to an investigation “relating to his functions . . . with respect to controlled substances.”⁶⁰ In Oregon, the Drug Enforcement Administration (“DEA”) had been attempting to use this administrative subpoena power to access the state’s PDMP data without a warrant.⁶¹ A United States Magistrate ordered the state to comply with the subpoena issued in this case, but Oregon responded by suing the Drug Enforcement Administration in federal district court.⁶² Oregon contended that its law requiring law enforcement to obtain a warrant before accessing PDMP data preempted the federal law allowing the Attorney General to issue administrative subpoenas during investigations.⁶³ The ACLU filed a Complaint in Intervention⁶⁴ with four patients and a doctor as plaintiffs,⁶⁵ but the Complaint in Intervention remained silent on the preemption issue.⁶⁶ The ACLU joined the suit only to enforce the plaintiff-interveners’ “Fourth Amendment rights to privacy in their protected health information.”⁶⁷ The court

⁵⁶ Frank Fernandez, *Attorney: Prescription Drug Database Unconstitutional*, DAYTONA BEACH NEWS-J. (June 12, 2013), <http://www.news-journalonline.com/article/20130612/NEWS/306129977>.

⁵⁷ *Or. Prescription Drug Monitoring Program v. DEA*, 998 F. Supp. 957 (D. Or. Mar. 31, 2013), available at https://www.aclu.org/files/assets/motion_to_intervene_granted.pdf (Order Granting Motion to Intervene).

⁵⁸ Gaston, *supra* note 18.

⁵⁹ OR. REV. STAT. § 431.966(2)(a)(D) (2014).

⁶⁰ 21 U.S.C. § 876(a) (2012).

⁶¹ Complaint in Intervention for Declaratory and Injunctive Relief at 3, *Or. Prescription Drug Monitoring Program v. DEA*, 998 F. Supp. 2d 957 (D. Or. 2014) (No. 3:12-cv-02023-HA), available at https://www.aclu.org/files/assets/2013.04.10_-_doc_18_-_complaint_in_intervention.pdf.

⁶² Gaston, *supra* note 18.

⁶³ *See id.*

⁶⁴ A complaint in intervention allows a party that was not originally part of a lawsuit to join the suit. *See* FED. R. CIV. P. 24.

⁶⁵ Complaint in Intervention, *supra* note 61, at 3–6.

⁶⁶ *See id.*

⁶⁷ *Id.* at 3–6, 12.

agreed with Oregon and the ACLU, ruling that the DEA could not use the administrative subpoena on Fourth Amendment grounds.⁶⁸

These cases illustrate one of the primary issues with PDMPs and raise important questions about the purpose and implementation of PDMPs. Some of these questions include: How can states effectively balance the privacy interests of patients against the interests of law enforcement in investigating the illegal use and distribution of prescriptions drugs? Can administrative subpoenas from federal agencies be used in place of a warrant in violation of state law? Should law enforcement have to obtain a warrant before accessing information even in states that do not require a warrant? Courts will have to apply at least some level of Fourth Amendment analysis when dealing with these questions. The following Part outlines the law this Note applies in its analysis in Parts IV–V.

III. THE APPLICABLE LAW: THE FOURTH AMENDMENT, HEALTHCARE-SPECIFIC PRIVACY LAWS, AND THE ADMINISTRATIVE SUBPOENA

This Part addresses the constitutional precedent, statutory provisions, and professional oath this Note applies in its analysis. First, Section A discusses general Fourth Amendment precedent. This discussion includes a description of what the Fourth Amendment protects, what constitutes a legitimate expectation of privacy, and what the government must show in order to conduct a search and/or seizure under the Fourth Amendment. Next, Section B examines Fourth Amendment precedent relating specifically to health information. Section C discusses extra-constitutional privacy protections for health information including HIPAA laws, doctor-patient privilege, and privacy protections included in state PDMP laws. Finally, Section D outlines the administrative subpoena power held by the Attorney General under the Controlled Substances Act, 21 U.S.C. § 876, and some court precedent relating to this power.

With these various laws, this Note will demonstrate, through its analysis in Part IV, that patients have a legitimate expectation of privacy in their personally identifiable PDMP data, and the Fourth Amendment requires that law enforcement obtain a warrant before accessing personally identifiable PDMP data. First, a general overview of the Fourth Amendment, what it protects, and how it protects.

A. *The Fourth Amendment Generally*

The Fourth Amendment of the United States Constitution guarantees citizens the right “to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures.”⁶⁹ The Supreme Court of the

⁶⁸ Or. Prescription Drug Monitoring Program v. DEA, 998 F. Supp. 2d 957, 967 (D. Or. 2014).

⁶⁹ U.S. CONST. amend. IV.

United States has consistently recognized that the Fourth Amendment, as well as other constitutional amendments, establishes an inferred right to privacy.⁷⁰ Indeed, as early as 1886 courts have held that the Fourth Amendment applies to “all invasions on the part of the government or its employees on the sanctity of a man’s home and the privacies of life.”⁷¹

The Fourth Amendment does not simply protect property or places from unreasonable searches and seizures; it also protects people, and its reach is not limited to physical intrusions into a private place.⁷² Privacy interests often involve a variety of more specific interests held by individuals, including “the individual interest in avoiding disclosure of personal matters, and . . . the interest in independence when making certain kinds of important decisions.”⁷³ PDMPs implicate the former of these interests by collecting and storing large quantities of information relating to these “personal matters.”

The Fourth Amendment “strikes a balance between individual citizen’s interest in conducting certain affairs in private, and general public’s interest in subjecting possible criminal activity to intensive investigation . . . by securing for each individual private enclave a ‘zone’ bounded by an individual’s own reasonable expectations of privacy.”⁷⁴ When a zone of privacy is implicated, courts must examine the exact governmental interests served and balance them against the specific invasion of privacy.⁷⁵

This privacy analysis will only apply if the individual has a legitimate expectation of privacy.⁷⁶ An individual’s subjective expectation of privacy is legitimate if it is “one that society is prepared to recognize as [objectively] ‘reasonable.’”⁷⁷ The legitimate expectation of privacy must also have a source beyond the Fourth Amendment, “either by reference to the concepts of real or personal property law or to understandings that are recognized and permitted by society.”⁷⁸ To determine whether an asserted privacy interest is reasonable, the court considers whether the person invoking the protection “took normal

⁷⁰ See *Time, Inc. v. Hill*, 385 U.S. 374, 411–20 (1967) (Fortas, J., dissenting) (citing several cases identifying a right to privacy, including *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Mapp v. Ohio*, 367 U.S. 643 (1961); *Wolf v. Colorado*, 338 U.S. 25, 28–29 (1949); *Olmstead v. United States*, 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting); and *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

⁷¹ *Boyd*, 116 U.S. at 630.

⁷² *Id.*

⁷³ *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

⁷⁴ *Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1042–43 (D.C. Cir. 1978), *cert. denied*, 440 U.S. 949 (1979).

⁷⁵ *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 671 (1989).

⁷⁶ *Minnesota v. Olson*, 495 U.S. 91, 95 (1990) (quoting *Rakas v. Illinois* 439 U.S. 128, 143 (1978)).

⁷⁷ *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

⁷⁸ *Rakas*, 439 U.S. at 143 n.12.

precautions to maintain his privacy—that is, precautions customarily taken by those seeking privacy.”⁷⁹

The Court has also been steadfast in its assertion that such privacy rights are not absolute.⁸⁰ States may make certain reasonable intrusions into these rights in the furtherance of a legitimate government interest.⁸¹ Typically, a search or seizure must be supported by a warrant issued upon a showing of probable cause.⁸² There are some exceptions to this requirement, such as the “exigent circumstances”⁸³ exception commonly used in the context of traffic stops⁸⁴ or the “special needs” exception invoked when the search serves government interests “beyond the normal need for law enforcement.”⁸⁵ One example of a situation where an “intrusion serves governmental needs, beyond normal need for law enforcement” is suspicionless urine testing to detect drug use in customs employees.⁸⁶ The government is also able to assert additional interests, beyond the normal need for law enforcement, in the context of administrative searches, where the regulated entity has a lessened expectation of privacy, and the government’s interest in the regulatory scheme outweigh any expectation of privacy that may exist.⁸⁷

Thus, the Fourth Amendment protects an individual’s privacy, and prevents the government from making arbitrary intrusions into both physical and intangible “zones of privacy.” This usually means law enforcement must get a warrant before invading such a zone, but this requirement and the Fourth Amendment rights underlying it are not absolute. These rights have often been applied to the doctor-patient relationship and health or healthcare information in general, specifically with regard to laws prohibiting and regulating

⁷⁹ *Id.* at 152; *see also* *United States v. Smith*, 621 F.2d 483, 487 (2d Cir. 1980), *cert. denied*, 449 U.S. 1086 (1981) (citing *Rakas*, 439 U.S. at 144 n.12, 152–53).

⁸⁰ *See, e.g., Von Raab*, 489 U.S. at 656; *Torres v. Puerto Rico*, 442 U.S. 465 (1979); *Roe v. Ingraham*, 364 F. Supp. 536 (S.D.N.Y. 1973).

⁸¹ *See e.g., Von Raab*, 489 U.S. at 656; *Torres*, 442 U.S. at 465; *Roe*, 364 F. Supp. at 536.

⁸² *Terry v. Ohio*, 392 U.S. 1, 20 (1968).

⁸³ Exigent circumstances are defined for the purpose of this Note as “a situation in which a police officer must take immediate action to effectively make an arrest, search, or seizure for which probable cause exists, and thus may do so without first obtaining a warrant.” BLACK’S LAW DICTIONARY 296 (10th ed. 2014). The most common example of exigent circumstances are searches of vehicles during traffic stops. A police officer with probable cause may search a vehicle without first getting a warrant. *See United States v. Ross*, 456 U.S. 798 (1982).

⁸⁴ *Ross*, 456 U.S. at 798, 799–800, 816.

⁸⁵ *Skinner v. Ry. Labor Execs. Ass’n*, 489 U.S. 602, 651–52 (1989) (Marshall, J., dissenting) (internal quotation marks omitted).

⁸⁶ *Von Raab*, 489 U.S. at 665–66.

⁸⁷ *See Donovan v. Dewey*, 452 U.S. 594 (1981) (allowing periodic warrantless inspections of underground mines by federal inspectors pursuant to the Federal Mine Safety and Health Act of 1977).

abortions,⁸⁸ laws requiring doctors to report treatment information to receive public healthcare funds,⁸⁹ laws establishing PDMPs,⁹⁰ and programs that disclose medical information to law enforcement.⁹¹

B. *The Fourth Amendment and Medical Information*

Courts have typically held that individuals have a legitimate expectation of privacy in their healthcare information. Once the court finds that a zone of privacy or legitimate expectation of privacy exists, the court must balance the asserted government interest against the specific invasion of privacy.⁹² Courts will examine several factors relating to the invasion of privacy to determine the extent of the intrusion and whether the intrusion is reasonable in light of the expectation of privacy or it is outweighed by it.⁹³ Certain places, activities, or information in which individuals have a *heightened* expectation of privacy trigger a presumption under the Fourth Amendment that law enforcement must obtain a warrant before intruding on one of those zones, allowing courts to dispense with the balancing test all together.⁹⁴ However, it is reasonable to infer that this presumption still represents a balancing of the state interests against the invasion of privacy⁹⁵—a balancing, in which the government has an extremely difficult burden to overcome if it hopes to circumvent the warrant requirement.⁹⁶ Still, not all government officials are

⁸⁸ See *Thornburgh v. Am. Coll. of Obstetricians and Gynecologists*, 476 U.S. 747 (1986), *overruled on other grounds by* *Planned Parenthood of Se. Pa. v. Casey*, 505 U.S. 833 (1992) (invalidating parts of a Pennsylvania law on Fourth Amendment grounds because the law required the collection of specific information about women receiving abortions, which could lead to their identification, and the information was made available to the public). *But see* *Roe v. Wade*, 410 U.S. 113 (1973). The Court in *Roe v. Wade* did not base its decision on the Fourth Amendment, but rather on other forms of privacy rights secured by the Fourteenth and Ninth Amendments. *Id.*

⁸⁹ See *Ass'n of Am. Physicians & Surgeons v. Weinberger*, 395 F. Supp. 125, 136–37 (N.D. Ill. 1975), *aff'd*, 423 U.S. 975 (1975). The Court in *Weinberger* applied the Fourth Amendment, but upheld the disclosure of information for a variety of reasons discussed *infra* in part III.B.

⁹⁰ See *Whalen v. Roe*, 429 U.S. 589, 598 & n.23 (1977). The Court upheld the PDMP program in *Whalen*, but only addressed the collection and maintenance of the PDMP data by the state, not disclosure to law enforcement. *Id.* at 603–04. Justice Brennan indicated in his concurrence that the Fourth Amendment may need to be applied in the future to limit the program. *Id.* at 606–07 (Brennan, J., concurring).

⁹¹ See *Ferguson v. City of Charleston*, 532 U.S. 67, 75–86. (2001).

⁹² *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 671 (1989).

⁹³ *Weinberger*, 395 F. Supp. at 136.

⁹⁴ *Or. Prescription Drug Monitoring Program v. DEA*, 998 F. Supp. 2d 957, 963–68, 965 n.3 (D. Or. 2014).

⁹⁵ See *id.* at 967–68.

⁹⁶ See *id.* at 963–68; see also *Ferguson*, 532 U.S. at 75–86; *Tucson Woman's Clinic v. Eden*, 379 F.3d 531, 549–53 (9th Cir. 2004).

required to obtain a warrant before receiving disclosures of information in which individuals have a heightened expectation of privacy.⁹⁷

Courts have reasoned 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.”⁹⁸ Requiring such warrantless disclosures to state representatives in charge of public health “does not automatically amount to an impermissible invasion of privacy.”⁹⁹ When determining whether an intrusion into private medical information is reasonable, courts have examined whether the information was sought for a legitimate governmental purpose, the manner in which the information was gathered and maintained, and whether confidentiality is protected.¹⁰⁰ Courts can then balance these factors to determine whether the asserted government interests outweigh the legitimate expectation of privacy.¹⁰¹

The state’s collection and disclosure of medical information is not a per se violation of the Fourth Amendment, and this principle allows for the existence of PDMPs in the first place.¹⁰² The Supreme Court in *Whalen v. Roe*¹⁰³ dealt with the New York State Controlled Substances Act of 1972, which included a provision that functioned as a PDMP.¹⁰⁴ The Supreme Court placed special importance on the fact that sufficient protections existed to keep private information from being disclosed to the public.¹⁰⁵ The same principles apply when the government collects healthcare information before dispensing Medicare and Medicaid funds.¹⁰⁶ The Supreme Court affirmed a federal district

⁹⁷ See *Whalen v. Roe*, 429 U.S. 589, 602 (1977).

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ *Ass’n of Am. Physicians & Surgeons v. Weinberger*, 395 F. Supp. 125, 135–38 (N.D. Ill. 1975), *aff’d*, 423 U.S. 975 (1975).

¹⁰¹ *Id.* at 137.

¹⁰² *Whalen*, 429 U.S. 589 (1977). The provision in *Whalen* required physicians to provide copies of prescription forms to the state health department, and the forms were required to identify the patients receiving Schedule II drugs in an effort to prevent the diversion of these drugs to illegal channels. *Id.* at 591–92. The Court held that the provision was not unreasonable because sufficient protections existed to keep private information from being disclosed to the public, and the requirement did not represent an intrusion on patient privacy. *Id.* at 600–02, 604. The Court quoted language in a footnote indicating its belief that the government interest in the reporting requirements outweighed any privacy interests that may have been compromised, if any. *Id.* at 601 n.27 (“[T]he substantial public interest in disclosure . . . outweighs the harm generally alleged.” (quoting *Buckley v. Valeo*, 424 U.S. 1, 71–72 (1976))).

¹⁰³ 429 U.S. 589 (1977).

¹⁰⁴ *Id.* at 591.

¹⁰⁵ *Id.* at 600–02, 604.

¹⁰⁶ *Ass’n of Am. Physicians & Surgeons v. Weinberger*, 395 F. Supp. 125, 135 (N.D. Ill. 1975). In *Weinberger*, the court addressed the constitutionality of the “Professional Standards

court decision allowing the federal government to collect information about patients to ensure the treatments they undergo are medically necessary and done in an economical manner.¹⁰⁷

In *Weinberger*, the court held that the government interests in controlling public expenditures related to healthcare were substantial enough to outweigh the doctors' and patients' privacy interests, particularly because there were adequate safeguards to ensure confidentiality.¹⁰⁸ The court also placed special importance on the fact that "[C]ongress simply [was] imposing a condition on the spending of public funds."¹⁰⁹ However, in the cases applying these principles, the courts did not address the disclosure of personal healthcare information to law enforcement.¹¹⁰

The Supreme Court did address the disclosure of medical information to law enforcement in *Ferguson v. City of Charleston*,¹¹¹ where the Court held that a patient who undergoes diagnostic tests has a reasonable expectation that the results of those tests will not be disclosed to nonmedical personnel without his or her consent.¹¹² In *Ferguson*, a public hospital in Charleston, South Carolina, disclosed the names of pregnant women who had tested positive for cocaine to police in an effort to use the threat of criminal prosecution to coerce the women into getting treatment.¹¹³ Here, the government asserted interests

Review" Legislation, which was intended to stem the rising costs of the Medicare and Medicaid Programs. *Id.* at 128–29. The law required doctors to furnish information about patients and treatments to a Professional Standards Review Organization ("PSRO") before receiving federal funds to pay for such treatments. *Id.* at 128–30. The PSRO used the information to create patient profiles to determine if the treatments were "medically necessary or could be provided for in a more economical manner." *Id.* at 130, 135. The plaintiff sought to have the law declared unconstitutional as a violation of rights protected by the First, Fourth, and Ninth Amendments. *Id.* at 131.

¹⁰⁷ *Id.* at 130, 136–38, *aff'd*, 423 U.S. 975 (1975).

¹⁰⁸ *Id.* at 130, 135–36. The law required the use of medical coding to ensure "maximum confidentiality and objective evaluation." *Id.* at 130. The court in *Weinberger* specifically addressed the Fourth Amendment privacy claims in its opinion, and the medical coding used weighed heavily in the government's favor during the analysis. *See id.* at 135–38.

¹⁰⁹ *Id.* at 138 (quoting *Cal. Banker's Ass'n v. Shultz*, 416 U.S. 21, 50 (1974)).

¹¹⁰ *See id.*; *Whalen v. Roe*, 429 U.S. 589, 589 (1977). Justice Brennan's concurrence in *Whalen* also stressed that the information was "made available only to a small number of public health officials with a legitimate interest in the information," and "[b]road dissemination by state officials of such information, however, would clearly implicate constitutionally protected privacy rights, and would presumably be justified only by compelling state interests." *Id.* at 606.

¹¹¹ 532 U.S. 67 (2001).

¹¹² *Id.* at 78.

¹¹³ *Id.* at 69–73, 79–81. The women were tested as part of their prenatal care, and there was a question as to whether the women consented to the information being turned over to law enforcement. *Id.* at 69, 75–76.

beyond the need for law enforcement for its policy to disclose the positive drug tests to law enforcement agencies.¹¹⁴

The Court closely scrutinized the scheme to disclose positive tests to law enforcement in *Ferguson*, and did not accept the government's asserted "special need" in "protecting the health of both mother and child."¹¹⁵ Furthermore, the Court distinguished the drug tests in *Ferguson* from other statutorily mandated disclosures by healthcare providers:¹¹⁶

The fact that positive test results were turned over to the police does not merely provide a basis for distinguishing our prior cases applying the "special needs" balancing approach to the determination of drug use. It also provides an affirmative reason for enforcing the strictures of the Fourth Amendment. While state hospital employees, like other citizens, may have a duty to provide the police with evidence of criminal conduct that they inadvertently acquire in the course of routine treatment, when they undertake to obtain such evidence from their patients *for the specific purpose of incriminating those patients*, they have a special obligation to make sure that the patients are fully informed about their constitutional rights, as standards of knowing waiver require.¹¹⁷

Although the Court emphasized the physician's purpose for obtaining the urine samples, the purpose only became impermissible when the hospital disclosed the results of the test to law enforcement.¹¹⁸ Prior to the formulation of the disclosure policy, the hospital was collecting and analyzing prenatal patients' urine if they met certain medical criteria that indicated potential cocaine use.¹¹⁹

¹¹⁴ *Id.* at 81.

¹¹⁵ *Id.* at 81–86. In coming to this conclusion the Court noted that the policy said nothing about different courses of treatment for the mother and child and was developed in close and constant collaboration with law enforcement. *Id.*

¹¹⁶ Doctors are often required by law to report crimes or threats to health and safety such as suspected child abuse, self-inflicted wounds, and threats made to third parties. *See Mental Health Professionals' Duty to Protect/Warn*, NAT'L CONF. OF ST. LEGS. (Jan. 2013), <http://www.ncsl.org/research/health/mental-health-professionals-duty-to-warn.aspx>; *see also* Noreen M. Grant, Note, *Psychiatrists Have No Duty to Warn Third Parties of Patients' Threats: Tarasoff is Kicked Out of Texas . . . Finally!*, 7 TEX. WESLEYAN L. REV. 157 (2001); Patricia C. Kussmann, Annotation, *Liability of Doctor, Psychiatrist, or Psychologist for Failure to Take Steps to Prevent Patient's Suicide*, 81 A.L.R.5th 167 (2000); Danny R. Veilleux, Annotation, *Validity, Construction and Application of State Statute Requiring Doctor or Other Person to Report Child Abuse*, 73 A.L.R.4th 782 (1989).

¹¹⁷ *Ferguson*, 532 U.S. at 84–85 (emphasis in original).

¹¹⁸ *See id.* at 85–86.

¹¹⁹ Schuyler Frautschi, *Understanding the Public Health Policies Behind Ferguson*, 27 N.Y.U. REV. L. & SOC. CHANGE 587, 588–90 (2001–02).

The Court held that because the “immediate objective” of the disclosures was to obtain evidence for “*law enforcement purposes*, . . . [t]he Fourth Amendment’s general prohibition against nonconsensual, warrantless, and suspicionless searches” applied.¹²⁰

The District Court in the Oregon case, discussed *supra* in Part II.C, dealt specifically with law enforcement access to state PDMPs.¹²¹ The court easily found that patients’ “subjective expectation of privacy in their prescription information is objectively reasonable.”¹²² In coming to its conclusion, the court in the Oregon case cited various sources of privacy protection for health information.¹²³ The court qualified the right, indicating that access by medical personnel was allowed, but stated, “[I]t is more than reasonable for patients to believe that law enforcement agencies will not have unfettered access to their records.”¹²⁴

The court cited this legitimate expectation of privacy as grounds for denying the DEA’s argument that the “third party doctrine”¹²⁵ should apply, distinguishing the cases in which that doctrine did apply.¹²⁶ The court concluded that the DEA could not use an administrative subpoena, in lieu of a warrant, to obtain Oregon’s PDMP data.¹²⁷ Without invoking the use of a balancing test, the court nevertheless concluded that the government’s asserted interests for using the administrative subpoena to access PDMP data did not outweigh the patient’s expectation of privacy in that data, and therefore, the use of the administrative subpoena in this way violated the Fourth Amendment.¹²⁸

¹²⁰ *Ferguson*, 532 U.S. at 82–83, 86 (emphasis in original). The Court specifically stated that the facts in *Ferguson* provided not only “a basis for distinguishing our prior cases applying the ‘special needs’ balancing approach It also provides an affirmative reason for enforcing the strictures of the Fourth Amendment.” *Id.* at 84. Indicating that the balance in this case shifted in favor of the patients, thus the government’s interest in the disclosure did not outweigh the patients’ expectation of privacy. *See id.* at 82–86.

¹²¹ *See Or. Prescription Drug Monitoring Program v. DEA*, 998 F. Supp. 2d 957, (D. Or. 2014).

¹²² *Id.* at 966.

¹²³ *Id.* at 964–65.

¹²⁴ *Id.* at 966.

¹²⁵ *Id.* at 966–68. The third party doctrine is discussed more fully *infra* in Part III.D. It is a standing doctrine that forecloses individuals from challenging subpoenas issued for or searches of a third-party’s records to which the individual being investigated may have disclosed incriminating information. *See sources cited infra* note 126.

¹²⁶ *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d at 966–68. *But see* *United States v. Miller*, 425 U.S. 435 (1976) (applying the doctrine to bank records); *United States v. Golden Valley Elec. Ass’n*, 689 F.3d 1108 (9th Cir. 2012) (applying the third party doctrine to the disclosure of utility records); *United States v. Phibbs*, 999 F.2d 1053, 1077 (6th Cir. 1993) (applying the doctrine to telephone and credit card statements).

¹²⁷ *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d at 967–68.

¹²⁸ *See id.* at 963–68.

Thus, warrantless disclosures of medical information to the state are not per se invalid, and these disclosures serve diverse regulatory functions such as monitoring prescription drugs and controlling public healthcare expenditures. However, patients still entertain a subjectively heightened, and objectively reasonable expectation of privacy in their healthcare information. Therefore, patients have a legitimate expectation of privacy in their personally identifiable PDMP data that is protected under the Fourth Amendment. The legitimate expectation of privacy that triggers Fourth Amendment protection is based on several sources of privacy protection for healthcare information discussed in the next Section, which indicate that the expectation is objectively reasonable.

C. Other Sources of Privacy Protection for Health Information

In addition to constitutional amendments, federal and state laws have addressed privacy issues concerning health information, including the “Privacy Rule” that accompanied the Health Insurance Portability and Accountability Act,¹²⁹ recognized doctor-patient privilege,¹³⁰ the various professional oaths taken by doctors, and privacy protections incorporated into the various state PDMP laws.¹³¹ These laws, and the professional oaths, reflect a general concern by citizens and healthcare providers regarding the privacy of their medical information. Through these measures, lawmakers and doctors have endeavored to ensure patients are honest and candid, and that they do not forego medical treatment due to privacy concerns.¹³²

The “Standards for Privacy of Individually Identifiable Health Information,” known as the HIPAA Privacy Rule, protects individually identifiable health information.¹³³ The rule was created to “assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care”¹³⁴ The rule prohibits disclosure of any health information that identifies the individual or “for which there is a reasonable basis to believe can

¹²⁹ See, e.g., 45 C.F.R. § 164 (2012); Kendra Gray, Note, *The Privacy Rule: Are We Being Deceived?*, 11 DEPAUL J. HEALTH CARE L. 89 (2008).

¹³⁰ *Maintaining Privacy of Health Information, in 50 STATE STATUTORY SURVEYS: HEALTH CARE: HEALTH CARE FACILITIES* (2013), available at 0100 SURVEYS 7 (Westlaw).

¹³¹ NAMSDL, *supra* note 21, at 37–38.

¹³² See Marie C. Pollio, Note, *The Inadequacy of HIPPA's Privacy Rule: The Plain Language Notice of Privacy Practices and Patient Understanding*, 60 N.Y.U. ANN. SURV. AM. L. 579 (2004), available at http://www.law.nyu.edu/sites/default/files/ccm_pro_064663.pdf.

¹³³ U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 1, 3–4 (2003), available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>.

¹³⁴ *Id.* at 1.

be used to identify the individual.”¹³⁵ The rule does allow for disclosure of the information to law enforcement in six circumstances, including, “as required by law,” which covers disclosures in response to court orders, warrants, and subpoenas.¹³⁶

While not all jurisdictions recognize a doctor-patient privilege, and no such privilege existed at common law, most states have adopted doctor-patient privilege by statute.¹³⁷ The privilege is held by the patient but may be invoked by a physician on behalf of a patient.¹³⁸ The privilege is not destroyed by the presence of medical personnel reasonably necessary to diagnose or treat the patient, close family or friends, or others whose presence the patient was unable to prevent.¹³⁹ The doctor-patient privilege protects communications as well as observations intended by the patient to be confidential and pursuant to diagnosis or treatment.¹⁴⁰

States also took patient privacy into account when creating their PDMPs, which is demonstrated by the many states that incorporated privacy protections into their PDMP laws. These measures include: exempting the data from public records laws; punishing the wrongful receipt, disclosure, or use of the information; and limiting who has access to the information.¹⁴¹ Public records laws, such as the Freedom of Information Act (“FOIA”), typically guarantee the public access to records produced through the normal business of government.¹⁴² The laws often include exemptions for certain kinds of records, which could include PDMP data,¹⁴³ but some states have chosen to include

¹³⁵ *Id.* at 3–4.

¹³⁶ *Id.* at 7. The six circumstances are as follows:

- (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests;
- (2) to identify or locate a suspect, fugitive, material witness, or missing person;
- (3) in response to a law enforcement official’s request for information about a victim or suspected victim of a crime;
- (4) to alert law enforcement of a person’s death, if the covered entity suspects that criminal activity caused the death;
- (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and
- (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

Id. (citing 45 C.F.R. §164.512(f) (2013)).

¹³⁷ 2 CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 5:42 (3d ed. 2007).

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ NAMSDDL, *supra* note 21, at 36–38.

¹⁴² *See, e.g.*, 5 U.S.C. § 552 (2012); FLA. STAT. § 119.011(12) (2013); W. VA. CODE § 29B-1-2(4) (2013).

¹⁴³ *See* 5 U.S.C. §§ 552(b)(1)–(9).

specific exemptions in their PDMP legislation.¹⁴⁴ In addition, some states make it a crime or impose civil fines when unauthorized users access PDMP information or when authorized or unauthorized users wrongfully use or disclose the information.¹⁴⁵ Finally, all states restrict access to PDMP data by designating and licensing narrow classes of authorized users.¹⁴⁶ The National Alliance for Model State Drug Laws¹⁴⁷ recommends these measures to help ensure confidentiality in state PDMPs.¹⁴⁸

Finally, not all sources of privacy protection for healthcare information are derived from the law. The professional oaths taken by healthcare providers, often variations of the Hippocratic Oath, specifically address patient privacy: “What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.”¹⁴⁹ Again, this confidentiality aspect of the oaths seeks to ensure patients are candid and honest with their healthcare providers and to protect those patients in vulnerable positions.¹⁵⁰

All of these laws reflect society’s general acceptance of the idea that medical information merits protection under the law. But other laws reflect society’s acceptance of the notion that, in some cases, law enforcement must be empowered to investigate crimes without a strict application of the Fourth Amendment. Typically, under the Fourth Amendment and subject to the exceptions described in Part III.A, law enforcement must obtain a warrant before conducting a search or seizure. However, Congress provided the Attorney General with a broad subpoena power to investigate violations of the Controlled Substances Act, which may act in the stead of a warrant in some circumstances.

D. *The Administrative Subpoena*

The administrative subpoena power at issue in the Oregon PDMP case, discussed *supra*,¹⁵¹ is an atypically broad grant of power to an agency.¹⁵²

¹⁴⁴ NAMSDDL, *supra* note 21, at 15.

¹⁴⁵ *Id.* at 37.

¹⁴⁶ *Id.* at 14.

¹⁴⁷ The National Alliance for Model State Drug Laws was formed by Congress in 1993 as the President’s Commission on Model State Drug Laws to create a model code of laws to help states deal with alcohol and drug abuse. *History*, NAT’L ALLIANCE FOR MODEL ST. DRUG LAWS, <http://www.namsdl.org/history.cfm> (last visited Oct. 15, 2014).

¹⁴⁸ NAMSDDL, *supra* note 21, at 15.

¹⁴⁹ See Peter Tyson, *The Hippocratic Oath Today*, NOVA (Mar. 27, 2001), <http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html>.

¹⁵⁰ *Id.*

¹⁵¹ See *supra* Part II.C.

However, courts have held that this power, clearly granted by Congress to a law enforcement official, is not invalid simply because it departs from the typical probable cause requirement in criminal investigations.¹⁵³ In *United States v. Hossbach*,¹⁵⁴ a Pennsylvania district court was reluctant to overturn the law permitting administrative subpoenas under the Controlled Substances Act.¹⁵⁵ The court felt it was within the legislature's power to pass the law, despite strong historical precedent that indicated such subpoenas should not be valid in criminal investigations.¹⁵⁶ Thus, the administrative subpoena power granted by 21 U.S.C. § 876, is not a per se violation of the Fourth Amendment.¹⁵⁷

Still, the courts have not completely abandoned the Fourth Amendment analysis when determining the validity of an administrative subpoena. For example, the Ninth Circuit held that administrative subpoenas can be constitutionally valid, analogizing them to Grand Jury subpoenas that may be issued only on suspicion that a crime has been committed or for assurance that the crime has not been committed.¹⁵⁸ However, this circuit has only upheld subpoenas in situations addressing records in which an individual has no legitimate expectation of privacy, such as business records.¹⁵⁹

The Sixth Circuit has held similarly, applying the "third party doctrine" to find that individuals do not have standing to dispute an administrative subpoena issued to a third-party on Fourth Amendment grounds where that individual has no "actual and justifiable privacy interest" in the records

¹⁵² See *United States v. Hossbach*, 518 F. Supp. 759, 767 (E.D. Pa. 1980).

¹⁵³ *Id.*

¹⁵⁴ *Id.*

¹⁵⁵ *Id.* at 766–67.

¹⁵⁶ *Id.*

¹⁵⁷ See *id.*

¹⁵⁸ *United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108, 1115–16 (9th Cir. 2012) (citing *United States v. Morton Salt Co.*, 338 U.S. 632, 642 (1950)). In *Golden Valley*, the DEA subpoenaed information from an energy cooperative about energy consumption by three of its customers as part of a criminal investigation for suspected violations of the Controlled Substances Act. *Id.* at 1111. The agents suspected the customers' residences were being used to grow marijuana under artificial lights. *Id.* at 1114 ("[E]lectricity consumption can indicate whether a person is growing marijuana because 'grow lamps necessitat[e] a large amount of electricity.'"). The court in *Golden Valley* pointed out that the information sought in that case consisted of business records in which the customers, the subjects of the investigation, had no reasonable expectation of privacy. *Id.* at 1116–17.

¹⁵⁹ *Id.* at 1116. By basing its Fourth Amendment ruling on the lack of a legitimate expectation of privacy, the court left the door open for lower courts in the Ninth Circuit to invalidate subpoenas that seek information in which the subject individuals may have a legitimate expectation of privacy. *Id.* ("Depending on the circumstances or the type of information, a company's guarantee to its customers that it will safeguard the privacy of their records might suffice to justify resisting an administrative subpoena.").

obtained.¹⁶⁰ Thus, courts have entertained challenges to administrative subpoenas on Fourth Amendment grounds, even if they usually have stopped short of invalidating them. In contrast, a district court in the Ninth Circuit specifically refused to allow the DEA to use an administrative subpoena to access PDMP data because of the legitimate expectation of privacy associated with the data.¹⁶¹

The Sixth Circuit case where the court applied the third-party doctrine, *United States v. Phibbs*,¹⁶² also discussed the administrative subpoena power, warrants, and the judicial process required for the issuance or enforcement of either.¹⁶³ The administrative subpoena does not completely abandon judicial process in its administration.¹⁶⁴ However, the standard used to enforce administrative subpoenas *duces tecum*¹⁶⁵ is not as strict as those used to issue a warrant.¹⁶⁶ If it is a subpoena *duces tecum*, “the subpoenaed party [must be able to] obtain judicial review of the reasonableness of the demand before suffering penalties for refusing to comply.”¹⁶⁷ But, if an on-premises search is required to execute the subpoena, and the sole purpose of the subpoena is to gather evidence for a criminal investigation, a warrant is required before the subpoena

¹⁶⁰ *United States v. Phibbs*, 999 F.2d 1053, 1077–78 (6th Cir. 1993) (citing *United States v. Miller*, 425 U.S. 435, 440–41 (1976)), *cert. denied*, 510 U.S. 1119 (1994). In *Phibbs*, one of the codefendants, Victor Rojas, challenged the validity of a subpoena used by the DEA to obtain his telephone records and credit card statements. *Id.* at 1076–78. The Sixth Circuit invoked the “third-party” doctrine applied in *Miller*, where the defendant had “no protectable Fourth Amendment interest” in his bank records. *United States v. Miller*, 425 U.S. 435, 436–40 (1976) (citing *United States v. White*, 401 U.S. 745, 752 (1971)) (“[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities[.]”). The third-party doctrine applies “even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.” *Id.* Thus, the court in *Phibbs* held that the defendant did not have standing to dispute an administrative subpoena issued to a third party on Fourth Amendment grounds, because the defendant had no “actual and justifiable privacy interest” in the records obtained. *Phibbs*, 999 F.2d at 1077–78.

¹⁶¹ *Or. Prescription Drug Monitoring Program v. DEA*, 998 F. Supp. 2d 957, 961 (D. Or. 2014).

¹⁶² *Phibbs*, 999 F.2d at 1053.

¹⁶³ *Id.* (The analysis of the standards required for administrative subpoenas in *Phibbs* is only dicta; however, because the court disposed of these issues on standing grounds rather than the merits of the petitioner’s constitutional claims.)

¹⁶⁴ *Id.* at 1077.

¹⁶⁵ A subpoena *duces tecum* is “a subpoena ordering the witness to appear in court and to bring specified documents, records, or things.” BLACK’S LAW DICTIONARY 1563 (9th ed. 2009).

¹⁶⁶ See *Phibbs*, 999 F.2d at 1077 (The subpoena has to be “sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance [would] not be unreasonable.” (quoting *See v. City of Seattle*, 387 U.S. 541, 544 (1967))).

¹⁶⁷ *Id.* (internal quotation marks omitted).

can be served.¹⁶⁸ This clearly demonstrates that administrative subpoenas *duces tecum* do not require a showing of probable cause, as warrants do.

A search warrant must meet similar standards of reasonableness relating to its scope, purpose, and specificity, but law enforcement must also show probable cause: “[a] reasonable ground . . . that a person has committed or is committing a crime, or that a place contains specific items connected with a crime.”¹⁶⁹ There must be “individualized suspicion of wrongdoing.”¹⁷⁰ This condition requires the agent or officer to attest to facts that demonstrate *why* the search should be permitted.¹⁷¹ The reasonableness standard for administrative subpoenas does not require this showing of *why* the search should be permitted, only that the search itself and *what* will be searched or disclosed is reasonable.¹⁷²

To summarize, the Fourth Amendment protects individuals from warrantless intrusions into specific zones of privacy, created by the individual’s reasonable expectation of privacy. The Fourth Amendment does not foreclose warrantless disclosures of medical information when the government can assert needs beyond the normal need for law enforcement, but the normal need for law enforcement will not suffice, on its own, to justify warrantless disclosures. In addition, the government interest must outweigh the expectation of privacy. Privacy protections for healthcare information exist outside of Fourth Amendment precedent in the form of statutes and the Hippocratic Oath which demonstrates that an expectation of privacy in this information is objectively reasonable. Finally, the administrative subpoena power is a valid grant of congressional power to the executive that allows some warrantless disclosures of information to law enforcement, but this power is not enough to overcome a legitimate expectation of privacy protected by the Fourth Amendment.

The next Part applies the various laws discussed in this Part to determine if individuals have a legitimate, and possibly heightened, expectation of privacy in their PDMP data to justify Fourth Amendment protection. Through this application, this Note shows that patients’ have a legitimate expectation of privacy in their personally identifiable PDMP data, and the Fourth Amendment requires that law enforcement obtain a warrant before accessing personally identifiable PDMP data.

¹⁶⁸ *Id.*

¹⁶⁹ BLACK’S LAW DICTIONARY 1321 (9th ed. 2009).

¹⁷⁰ *Chandler v. Miller*, 520 U.S. 305, 312 (1997).

¹⁷¹ *See* FED. R. CRIM. P. 41.

¹⁷² *See Phibbs*, 999 F.2d at 1077.

IV. A PATIENT'S LEGITIMATE EXPECTATION OF PRIVACY IN PDMP DATA JUSTIFIES A WARRANT REQUIREMENT

This Part argues that law enforcement must obtain a warrant before accessing personally identifiable PDMP data. The purposes of state PDMPs are somewhat varied.¹⁷³ Ultimately, the programs are intended to help states regulate controlled substances and prevent abuse of these substances by providing prescribers, dispensers, and law enforcement with the information necessary to identify individuals that may be diverting prescription drugs from legitimate channels to sell or use illicitly.¹⁷⁴ However, states must balance the various means used to achieve these various purposes against the patients' expectations of privacy. When law enforcement agents seek access to PDMP data for the purpose of enforcing drug laws, states must require them to obtain a warrant to ensure that innocent individuals do not have their private medical information needlessly disclosed and disseminated. Furthermore, states should make sure that, even with a valid warrant or valid warrantless access (by a doctor, nurse, or pharmacist), the subsequent wrongful dissemination and disclosure of PDMP data is punishable by criminal and/or civil penalties, and that PDMP data is specifically exempted from public records laws.

In this Part, Section A discusses why patients have a legitimate expectation of privacy in their prescription information, Section B discusses why law enforcement must obtain a warrant before accessing this information, and Section C discusses why states should include additional privacy protections in their PDMPs beyond the warrant requirement for law enforcement.

A. Patients Have a Legitimate Expectation of Privacy in Their PDMP Data

Prescription information, like other healthcare information, is inherently personal.¹⁷⁵ Patients often do not discuss these issues publicly, and in many cases, the information may be embarrassing or potentially damaging to one's reputation.¹⁷⁶ The information is typically only exchanged within relationships that society has begun to recognize as privileged: those relationships between doctors and patients.¹⁷⁷ The following subsections will explain why patients have a subjective expectation of privacy in their prescription information, and why this expectation is objectively reasonable.

¹⁷³ See NAMSDDL, *supra* note 21, at 11; see also *supra* note 25.

¹⁷⁴ NAMSDDL, *supra* note 21, at 11; see also *supra* note 25.

¹⁷⁵ Complaint in Intervention, *supra* note 61.

¹⁷⁶ *Id.* at 19.

¹⁷⁷ See 2 CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 5:42 (3d ed. 2007).

The analysis will also argue why extra-constitutional sources of privacy protection for health information have bolstered these arguments.¹⁷⁸

1. Patients Have a Subjective Expectation of Privacy in Their PDMP Data

The first level of analysis must determine whether the individual raising Fourth Amendment privacy issues has a subjective expectation of privacy in the information that will be the subject of the search.¹⁷⁹ When applied to a physical search, courts have held that individuals have a subjective expectation of privacy in their homes.¹⁸⁰ With regard to medical information, courts have usually found that a subjective expectation of privacy exists.¹⁸¹

A subjective expectation is easy to assert so long as the individual “took normal precautions to maintain his privacy.”¹⁸² Such precautions—which in the case of healthcare information would likely mean not discussing your personal health information publicly or not disclosing it to individuals beyond healthcare providers, family, and very close friends—represent a subjective expectation by the patient that their health information will remain private.

Therefore, it is clear that courts recognize that patients often, if not always, maintain some subjective expectation of privacy in their medical information. The subjective expectation of privacy is not controlling, however, and its presence or absence will not determine whether the Fourth Amendment applies. Its presence or absence only determines whether the first prong of the test is satisfied. The subjective expectation must also be objectively reasonable.¹⁸³

2. Society Is Prepared To Recognize this Expectation as Objectively Reasonable

Once the subjective expectation of privacy is asserted, the court must determine whether this expectation is objectively reasonable. An expectation of privacy must be “reasonable in light of all the surrounding circumstances.”¹⁸⁴

¹⁷⁸ See *supra* Part III.C.

¹⁷⁹ See *Minnesota v. Olson*, 495 U.S. 91, 95–96 (1990) (citing *Rakas v. Illinois*, 439 U.S. 128, 143 (1978); *Katz v. United States*, 389 U.S. 347, 361 (1967)).

¹⁸⁰ See *id.*

¹⁸¹ See *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (patients undergoing diagnostic tests in a hospital enjoy a reasonable expectation of privacy, such that the results of such tests will not be shared with nonmedical personnel without consent).

¹⁸² See *Rakas*, 439 U.S. at 152 (Powell, J., concurring).

¹⁸³ *Id.*

¹⁸⁴ *Id.*

Several factors may be considered when determining whether an expectation of privacy is reasonable, including “the precautions a person takes to maintain his privacy, the way he uses a location, the history of the Fourth Amendment, the property interests involved, and society’s recognition of customary behavior.”¹⁸⁵ This analysis is most often applied to physical searches but could also be applied to the disclosure of information.¹⁸⁶

With regard to the disclosure of information, the Supreme Court “has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.”¹⁸⁷ This “third party” doctrine applies “even if the information is revealed on the assumption that it will be used for a limited purpose and the confidence placed in the party will not be betrayed.”¹⁸⁸ This reasoning stands somewhat at odds with *Ferguson*, where urine was turned over by patients to third-party doctors as part of prenatal treatment but the subsequent urinalysis results could not be used as evidence for criminal prosecution without the patients’ consent or a warrant.¹⁸⁹ But the distinction becomes clear if one examines the cases in which this “third-party” exception was applied, because those cases dealt with information not typically associated with privacy rights, such as bank records.¹⁹⁰

Medical information is clearly distinguishable from bank records, as are the government interests in obtaining either. Bank records differ from PDMP data because the health information PDMP data contains is “more

¹⁸⁵ *United States v. Smith*, 621 F.2d 483, 487 (2d Cir. 1980) (citing *Rakas*, 439 U.S. at 152–53 n.12), *cert. denied*, 449 U.S. 1086 (1981).

¹⁸⁶ To the extent the factors presented in *Smith* can be applied to a disclosure of information, the fact that no physical search was involved does not matter because “[e]xpectations of privacy protected by the Fourth Amendment, of course, need not be based on a common-law interest in real or personal property, or on the invasion of such an interest.” *Rakas*, 439 U.S. at 143–44 n.12. Therefore, it is a logical conclusion that factors a court uses to determine whether a legitimate expectation of privacy exists within the context of a physical invasion of person or property could be used to evaluate the legitimacy of an expectation outside the context of a physical invasion of person or property, excluding factors specifically relating to a physical location. For example, a person who does not openly discuss his medical conditions is taking precautions to “maintain his privacy,” and as discussed *infra* in Part IV.A.2, society recognizes this “behavior” as reasonable if not “customary.” *Smith*, 621 F.2d at 487; *see also Ferguson*, 532 U.S. at 84–85.

¹⁸⁷ *United States v. Miller*, 425 U.S. 435, 443 (1976) (citing *United States v. White*, 401 U.S. 745, 751–52 (1971); *Hoffa v. United States*, 385 U.S. 293, 302 (1966); *Lopez v. United States*, 373 U.S. 427, 447–51 (1963) (stating that expressing a thought or message to a third party is a risk the speaker takes that the information may be discoverable)).

¹⁸⁸ *Id.*

¹⁸⁹ *See Ferguson*, 532 U.S. at 84–85.

¹⁹⁰ *See Miller*, 425 U.S. at 440–44.

inherently personal or private than [the information in] bank records,¹⁹¹ and are entitled to and treated with a heightened expectation of privacy.”¹⁹¹

Furthermore, the relationship between doctor and patient is much different than the relationship between the banker and the depositor.¹⁹² If a patient cannot opt out of having their prescription data collected for a PDMP (mandatory participation is a commonly recommended practice),¹⁹³ then the only way to avoid submission of prescription information to . . . PDMP[s] is to forgo medical treatment . . .”¹⁹⁴ A bank transaction is entirely voluntary. Individuals can hoard their money under their mattresses without jeopardizing their life or happiness, but medical treatment, because it is often necessary for life or happiness, forces patients to seek out doctors. Simply put, “patients and doctors are not voluntarily conveying information to the PDMP.”¹⁹⁵

Strong policy considerations back up the assertion that medical information disclosed and discussed between a doctor and a patient should not be subject to unconsented, warrantless disclosures.¹⁹⁶ As discussed in the next sub-section, several sources of privacy protection beyond the Fourth Amendment illustrate these policy considerations and bolster the argument that patients have an objectively reasonable expectation of privacy in their PDMP data.

3. Privacy Expectations for Health Information, Including PDMP Data, Have Sources Beyond the Fourth Amendment

Legitimate expectations of privacy must be derived from a source other than the Fourth Amendment.¹⁹⁷ Property rights were the earliest sources used to establish a legitimate expectation of privacy under the Fourth Amendment.¹⁹⁸ In the case of health information, there are many sources for an expectation of privacy beyond the Constitution. These sources include recognized doctor-patient privileges, the Privacy Rule accompanying the Health Insurance

¹⁹¹ *Or. Prescription Drug Monitoring Program v. DEA*, 998 F. Supp. 2d 957, 967 (D. Or. 2014) (quoting *United States v. Golden Valley Elec. Ass’n*, 689 F.3d 1116, 1116 (9th Cir. 2012)).

¹⁹² *See id.*

¹⁹³ *NAMSDL*, *supra* note 21, at 12, 14.

¹⁹⁴ *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d at 967 (“That is not a meaningful choice.”).

¹⁹⁵ *See id.*

¹⁹⁶ *See supra* Part III.C (regarding ensuring patients are honest and candid with healthcare providers).

¹⁹⁷ *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978).

¹⁹⁸ *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (2004).

Portability and Accountability Act (“HIPAA”), the Hippocratic Oath taken by doctors, and privacy protections accompanying the state PDMPs.¹⁹⁹

Although doctor-patient privileges did not exist at common law, they have developed over time in many states and operate like any other evidentiary privilege, barring individuals from testifying about those privileged matters.²⁰⁰ The privilege is justified by the need to preserve trust in the doctor-patient relationship.²⁰¹ This trust is important because it encourages patient candor, which is necessary for the proper diagnosis and treatment of disease or injury.²⁰² While HIPAA came about for many reasons, including improving communication of health information between providers and insurance entities, it also included a “privacy rule” to help protect this information from extensive disclosure and dissemination.²⁰³ Again, confidentiality is a central concern regarding healthcare information.

This confidentiality and the resulting trust are, in fact, central to the practice of medicine, as evidenced by the various professional oaths taken by physicians.²⁰⁴ The fact that many states have included additional privacy protections in their PDMPs, such as imposing criminal or civil punishments for wrongful disclosure of PDMP data, only further indicates a strong desire to keep healthcare information private, to promote patient candor.²⁰⁵

These various protections for patient privacy clearly indicate that this is an expectation of privacy society is prepared to recognize as reasonable.²⁰⁶ Patients are entitled to rely on Fourth Amendment holdings and laws such as HIPAA, and these laws provide objective support for the notion that society recognizes their subjective expectation as reasonable. Protecting the privacy of patients serves important policy functions, such as encouraging candor with healthcare providers and protecting individuals from embarrassment or judgment based on their health or medical choices. While some state interests

¹⁹⁹ See *supra* Part III.C.

²⁰⁰ MUELLER & KIRKPATRICK, *supra* note 137, § 5:42.

²⁰¹ See Anne D. Lampkin, *Should Psychotherapist-Patient Privilege Be Recognized?*, 18 AM. J. TRIAL ADVOC. 721 (1995).

²⁰² See *id.*

²⁰³ See Kevin B. Davis, *Privacy Rights in Personal Information: HIPAA and the Privacy Gap Between Fundamental Privacy Rights and Medical Information*, 19 J. MARSHALL J. COMPUTER & INFO. L. 535 (2001).

²⁰⁴ See Tyson, *supra* note 149. While the Tyson article points out that some have called the purpose and effectiveness of oaths in modern medicine into question, their prevalence and consistent inclusion of clauses requiring confidentiality demonstrates the importance privacy still holds in modern medicine. See Jessica De Bord et al., *Confidentiality*, UNIV. OF WASH. SCH. OF MED. (Mar. 6, 2014), <https://depts.washington.edu/bioethx/topics/confiden.html>.

²⁰⁵ See NAMSDEL, *supra* note 21, at 15, 37.

²⁰⁶ *Or. Prescription Drug Monitoring Program v. DEA*, 998 F. Supp. 2d 957, 964 (D. Or. 2014).

may warrant an intrusion into this privacy, the interest in law enforcement is not enough to permit such intrusions without a warrant.

B. Law Enforcement Must Show Probable Cause and Obtain a Warrant Before Accessing PDMP Data

As discussed above,²⁰⁷ this Note shows that individuals have a legitimate expectation of privacy in their medical information, but this does not end the Fourth Amendment analysis. Once a zone of privacy is implicated, the court must balance the specific intrusion and the government interests served by intruding on the zone against the specific privacy interest implicated.²⁰⁸ This Note addresses only disclosures of PDMP data to law enforcement serving government interests relating to the need for law enforcement.

1. The State's Interest in Law Enforcement Does Not Outweigh a Patient's Legitimate Expectation of Privacy in Their PDMP Data

The issue addressed in this Section is somewhat novel. The only case law that has been established relating specifically to law enforcement access to PDMP data is a district court case in Oregon,²⁰⁹ but existing Supreme Court precedent does suggest that PDMP data should not be subject to warrantless and unconsented access by law enforcement.²¹⁰ The case that most clearly supports this assertion is *Ferguson*, because it deals with warrantless law enforcement access to private health information.

In *Ferguson*, patients provided urine samples as part of their prenatal treatment, and samples that tested positive for cocaine were provided to law enforcement.²¹¹ The women in *Ferguson* were then threatened with arrest unless they entered drug treatment.²¹² In the case of PDMP data, the patients' prescription information is collected as part of their treatment for any number of conditions, and the data is kept by the state.²¹³ Although doctors may not be affirmatively providing PDMP information to law enforcement, as in *Ferguson*, allowing law enforcement to obtain the information without a warrant has the same effect: the warrantless, unconsented disclosure of private health

²⁰⁷ See *supra* Part IV.A.2.

²⁰⁸ Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665–66 (1989).

²⁰⁹ See *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d at 957.

²¹⁰ See *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001); *Thornburgh v. Am. Coll. of Obstetricians & Gynecologists et al.*, 476 U.S. 747, 774–76 (1986).

²¹¹ *Ferguson*, 532 U.S. at 70–76.

²¹² *Id.* at 70–74.

²¹³ See *NAMSDL*, *supra* note 21, at 6.

information purely for law enforcement purposes.²¹⁴ Furthermore, the government's interest in such disclosures does not outweigh the privacy interests of the patients.²¹⁵

It is more difficult for the government to assert interests beyond the normal need for law enforcement in a case involving law enforcement access to PDMP data, than it was to assert additional interests in *Ferguson*. First, in *Ferguson*, law enforcement had a unique coercive ability that they used in an attempt to protect the unborn children by getting their mothers off of drugs, and the healthcare providers were not succeeding in getting the women to stop using drugs on their own.²¹⁶ Second, the drugs in *Ferguson* were illegal drugs without legitimate medical uses—at least in the context that the women were using them—but doctors prescribe the drugs disclosed in PDMP data for legitimate medical uses.²¹⁷ Third, the doctors in *Ferguson* only turned over positive tests for an illegal drug.²¹⁸ With PDMP data, there is a much greater potential that innocent patients' data will be disclosed.²¹⁹ Finally, any interests in limiting the diversion and abuse of prescription drugs can be achieved by the physicians and pharmacists without law enforcement. A doctor can use the data to identify and deny drugs to a doctor-shopping patient, as may a pharmacist.²²⁰ The data could also be used to ensure patients are not receiving drugs in excess of reasonable therapeutic ranges without law enforcement accessing the data.²²¹

Certainly, the question arises as to whether a doctor should be obligated, or even allowed to disclose information about a patient's drug habits to law enforcement when he believes a patient is abusing drugs. Doctor-patient privilege would suggest a doctor should never be allowed to disclose this type of information to law enforcement,²²² and the ruling in *Ferguson* also seems to lead to the conclusion that disclosing such evidence of drug abuse to law enforcement should be forbidden without patient consent or a warrant.²²³ Conversely, doctors are often obligated to report evidence of issues such as domestic abuse, self-inflicted harm, or threats to third parties, but these obligations typically come into play to protect individuals from threats of

²¹⁴ See Kam, *supra* note 51.

²¹⁵ *Ferguson*, 532 U.S. at 84–86.

²¹⁶ *Id.* at 70–71.

²¹⁷ See *id.* at 70.

²¹⁸ *Id.* at 73.

²¹⁹ See Kam, *supra* note 51.

²²⁰ See Nick Budnick, *Hundreds of High-Prescribers Don't Check Oregon's Pharmacy-Monitoring Program*, OREGONLIVE (Dec. 18, 2012, 9:01 PM), http://www.oregonlive.com/health/index.ssf/2012/12/hundreds_of_high-prescribers_d.html.

²²¹ See Meier, *Painkiller Crackdown*, *supra* note 14.

²²² See MUELLER & KIRKPATRICK, *supra* note 137.

²²³ See *Ferguson*, 532 U.S. at 84–86.

imminent harm.²²⁴ Perhaps a doctor may have to alert authorities if he believes an overdose by one of his or her patients is imminent, but PDMPs contain information about patients that are not facing imminent harm. Thus, allowing law enforcement unwarranted access to PDMPs is not congruent with the other disclosure requirements.

While doctors' hands should not be tied when they suspect a patient is engaging in unlawful drug-seeking behavior or drug abuse, reporting such behavior to law enforcement would hopefully be a last resort. The need to report is lessened simply because the PDMP can allow pharmacists and prescribers to identify doctor-shoppers and deny them medication.²²⁵ Ideally, responsible physicians would try to get these patients to seek treatment, or supervise them through some form of a cessation program.²²⁶ Thus, any law that mandates disclosure of suspected drug abuse to law enforcement should not be necessary and would prevent doctors from pursuing other measures before tipping off law enforcement. The alternative method of using physicians and pharmacists to prevent drug abuse further illustrates law enforcement's limited interest in accessing PDMP data without a warrant.

Therefore, the only interest a law enforcement agency can assert when seeking access to PDMP data without a warrant is the need for law enforcement, and this need is not enough to overcome the patients' legitimate expectation of privacy in their health information protected by the Fourth Amendment.²²⁷ Furthermore, as discussed in the next Section, the administrative subpoena cannot displace a warrant with regard to this information.

2. Administrative Subpoenas Cannot Be Used To Obtain PDMP Data

The DEA has attempted to use the Attorney General's administrative subpoena power under 21 U.S.C. § 876 to access PDMP information without obtaining a warrant, despite state laws requiring warrants for law enforcement agents to access the information.²²⁸ While the administrative subpoena does not totally abandon judicial process, as the agency issuing the subpoena must seek a court order to have the subpoena enforced, the standard for such a ruling is less stringent than probable cause.²²⁹ Determining whether the subpoena is

²²⁴ See *supra* note 116.

²²⁵ See Budnick, *supra* note 221.

²²⁶ See Michael C. Barnes, Exec. Dir., Ctr. for Lawful Access and Abuse Deterrence, Legal Policy Strategies To Address an Evolving Epidemic (Feb. 13, 2014), available at <http://claad.org/wp-content/uploads/2014/02/CLAAD-WVU-140211-Compatibility-Mode.pdf>.

²²⁷ See *Ferguson*, 532 U.S. at 81–83.

²²⁸ Complaint in Intervention, *supra* note 61, at 10.

²²⁹ See *United States v. Phibbs*, 999 F.2d 1053, 1077 (6th Cir. 1993), *cert. denied*, 510 U.S. 1119 (1994).

reasonable, as is required for enforcement, has nothing to do with the issue of *why* the information was subpoenaed, only *what* the information subpoenaed was and whether the subpoena was narrow in scope, relevant in purpose, and specific.²³⁰

While the relevance requirement may provide some vague concept of why the subpoena should be enforced, it deals mostly with why the agent wants the information to further this specific investigation, not why they deserve to access the information. In essence, to get a judge to enforce an administrative subpoena, it is enough for an agent to say, hypothetically, “We need the suspect’s utility records because we are investigating him for growing marijuana, the subpoenaed party has easy access to those records and the number of records requested is not unreasonably large.”²³¹ On the other hand, to get a warrant the agent must say, “We need the suspect’s utility records because we are investigating him for growing marijuana, the subpoenaed party has easy access to those records, the number of records requested is not unreasonably large, and we know the suspect purchased several high-powered lights normally used for growing marijuana.”²³² The additional factual assertion about the lights in the second statement is the “full probable cause showing” necessary for the warrant.²³³

The Fourth Amendment’s probable cause requirement is designed to prevent arbitrary or groundless government searches for the purpose of gathering evidence for a criminal prosecution.²³⁴ If the government can conduct such searches without this showing, it opens the door for arbitrary and groundless searches, and gives the government the power to conduct searches for improper or nefarious reasons with little or no accountability. Requiring an agent to attest to facts necessary to establish probable cause allows for independent judicial analysis of those facts and provides an important check on the executive branch. The executive branch already has enormous investigative power, and if agents of the executive branch are allowed to sidestep the Fourth Amendment’s probable cause requirement simply because the evidence they want is relevant to an active investigation, “active investigations” may be broadly defined or “investigations” may be initiated simply to use such subpoenas in place of a warrant. Furthermore, when an agent attests to the facts

²³⁰ *Id.*

²³¹ *Cf.* *United States v. Golden Valley Elec. Ass’n*, 689 F.3d 1108, 1116 (9th Cir. 2012) (holding that an administrator’s investigative function is similar to a grand jury’s).

²³² *Cf. Phibbs*, 999 F.2d at 1077 (holding that valid search warrants are needed if consent is not forthcoming).

²³³ *Id.* (“If, as in the instant case, the subpoena is to be based on 21 U.S.C. § 876, ‘and the purpose behind the search [is] . . . a quest for evidence to be used in a criminal prosecution,’ a full probable cause showing is mandatory.” (citations omitted)).

²³⁴ *See* U.S. CONST. amend. IV.

necessary for probable cause in a sworn affidavit, if those facts turn out to be fabricated or mistakenly untrue, that agent faces accountability.²³⁵

While the probable cause requirement does not always apply in the context of administrative searches,²³⁶ patients are not under the administrative authority of the DEA. Patients are not regulated by the DEA, and the DEA would not be able to pursue civil punishments, such as revocation of a controlled substances license, against a patient. The DEA's only purpose for obtaining the information about patients is to enforce criminal laws against those patients, and in that context probable cause is required.²³⁷ The crux of this principle is that the government interest in executing searches for the purpose of administrative regulation outweighs the lessened privacy interests of the party that is the subject of the regulation.²³⁸

Furthermore, the administrative subpoena is traditionally limited to information in which the individual to be prosecuted has no legitimate expectation of privacy, such as phone, utility, and bank records.²³⁹ These records are considered business records "readily accessible to employees in the normal course of business[.]"²⁴⁰ unlike information about prescriptions which, are typically only accessible by certain employees as part of or during the provision of medical services due to HIPAA and PDMP laws.²⁴¹ In the case of PDMP data, the patient can assert privacy interests in the information, and thus the Fourth Amendment forecloses the use of an administrative subpoena to gather this information.

Finally, the government cannot assert any "exigent circumstances," or any other exception to the warrant requirement, that would excuse the lack of a warrant. PDMP data is not transient: it will not disappear in the time it takes law enforcement to get a warrant. There are no circumstances where law

²³⁵ See *Franks v. Delaware*, 438 U.S. 154, 171 (1978); see also *Kalina v. Fletcher*, 522 U.S. 118, 127–29 (1997).

²³⁶ See *Donovan v. Dewey*, 452 U.S. 594, 598 (1981) ("[U]nlike searches of private homes, which generally must be conducted pursuant to a warrant in order to be reasonable under the Fourth Amendment, legislative schemes authorizing warrantless administrative searches of commercial property do not necessarily violate the Fourth Amendment.").

²³⁷ See *Phibbs*, 999 F.2d at 1077 ("If, as in the instant case, the subpoena is to be based upon 21 U.S.C. § 876, 'and the purpose behind the search [is] . . . a quest for evidence to be used in a criminal prosecution,' a full probable cause showing is required." (quoting *United States v. Lawson*, 502 F. Supp. 158, 165 (D. Md. 1980))).

²³⁸ *United States v. Lawson*, 502 F. Supp. 158, 165 (D. Md. 1980) ("A lower standard of probable cause is constitutionally permissible in the administrative inspection context because the intrusion into an individual's privacy is less than that in the criminal context, and is outweighed by the public's interest in the regulatory program.").

²³⁹ *Phibbs*, 999 F.2d at 1077; see also *United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108 (9th Cir. 2012).

²⁴⁰ *Phibbs*, 999 F.2d at 1078.

²⁴¹ See 45 C.F.R. §§ 160.102, 160.516 (2006); NAMSDDL, *supra* note 21, at 26.

enforcement would need immediate access to prevent the threat of imminent harm, where a doctor or pharmacist could not as easily prevent that harm. Because law enforcement must obtain a warrant before accessing PDMP data, PDMPs that do not comply with this requirement must be declared unconstitutional.

3. State PDMPs That Allow Law Enforcement To Access the Data Without a Warrant Are Unconstitutional

As described *supra*,²⁴² state PDMPs vary in terms of the level of access they give law enforcement.²⁴³ While some states, such as Oregon, require law enforcement to obtain a warrant,²⁴⁴ others allow law enforcement to access the data at will,²⁴⁵ and others house their PDMPs within law enforcement agencies.²⁴⁶ This type of unfettered access to PDMP data by law enforcement violates patients' legitimate expectation of privacy in their health information. Again, these law enforcement entities cannot assert any interest in obtaining the information beyond the normal need for law enforcement, and this need alone does not outweigh a legitimate privacy interest.

If the above principles are to apply to PDMPs at all, they must apply to all PDMPs. Constitutionally protected privacy rights do not end at state borders, and allowing some states to disclose this private information to law enforcement without consent or a warrant violates the Fourth Amendment. Therefore, any state PDMP that allows law enforcement to access PDMP data without specific consent or a warrant are unconstitutional and must be brought into compliance with these principles.

In summary, individuals have a legitimate expectation of privacy in their health information, law enforcement must get a warrant before accessing PDMP data, and an administrative subpoena will not suffice. Because the Constitution applies to all the states, this principle applies regardless of what state law says, and law enforcement must get a warrant before accessing PDMP data, even where state law allows warrantless access. The next Section recommends that states employ additional privacy protections for PDMP data beyond the warrant requirement for law enforcement.

C. States Should Include Privacy Protection Within Their PDMPs

In addition to requiring law enforcement to obtain a warrant before accessing PDMP data, states should be encouraged to include additional

²⁴² See *supra* Part II.A.

²⁴³ NAMS DL, *supra* note 21, at 29.

²⁴⁴ *Id.*

²⁴⁵ See *id.*

²⁴⁶ *Id.* at 8.

privacy protections in their PDMPs. PDMP data is sometimes kept in electronic databases that could be vulnerable to cyber criminals.²⁴⁷ There is also the potential that unauthorized employees in doctors' offices, hospitals, and pharmacies could gain access to the information, and even authorized users may disclose or disseminate the information improperly.²⁴⁸ HIPAA laws do impose civil and criminal penalties on individuals that disclose personally identifiable health information,²⁴⁹ and in many ways, this may be a sufficient means of punishing individuals that improperly disclose PDMP data. Still, some states have included additional penalties within their PDMP laws that specifically apply to PDMP data.²⁵⁰

The advantages of including penalties within PDMP laws, beyond HIPAA laws, should not be understated. The federal government, through a relatively complex regulatory scheme, enforces HIPAA, a federal law.²⁵¹ The Department of Health and Human Services, Office of Civil Rights ("OCR") is in charge of ensuring that covered entities comply with HIPAA laws, and the OCR is also in charge of imposing civil penalties for noncompliance.²⁵² Criminal prosecutions under the HIPAA privacy rule are handled by the Department of Justice.²⁵³ These federal agencies are already spread very thin, and federal court dockets have little room for additional cases. Including penalties in state PDMPs empowers state governments to deal with improper use and disclosure of PDMP data. State courts could handle prosecutions, and civil or criminal fines could go back to the states to help fund their PDMPs. Therefore, states can benefit financially, and violations can be dealt with in a more efficient manner, if they include penalties within their PDMP laws. Additionally, states should explicitly exempt PDMP data from public records laws such as the Freedom of Information Act.²⁵⁴

It seems counter-intuitive that PDMP data would be subject to Freedom of Information Act ("FOIA") requests by the general public, but because the data is maintained by the state, and because PDMPs use public funds to operate, there is at least a cognizable argument that the data is a public record.²⁵⁵ Some states have addressed this by specifically exempting PDMP

²⁴⁷ NAMSDDL, *supra* note 21, at 6.

²⁴⁸ See Kam, *supra* note 51.

²⁴⁹ 42 C.F.R. § 3.418 (2012).

²⁵⁰ NAMSDDL, *supra* note 21, at 15.

²⁵¹ See Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 42 U.S.C.).

²⁵² See U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 133, at 3-4.

²⁵³ *Id.* at 18.

²⁵⁴ NAMSDDL, *supra* note 21, at 15.

²⁵⁵ See 5 U.S.C. § 552(f)(2) (2012).

data from public records requests.²⁵⁶ However, these additional protections may not be necessary due to exemptions already contained in public records laws.²⁵⁷ But a specific statutory exemption within the PDMP legislation ensures that the information is not subject to public records requests, and when individual privacy rights are implicated states should be encouraged to use any means necessary to protect these rights.

These additional privacy protections, while not entirely necessary, could help quell fears that PDMPs have created relating to patient privacy.²⁵⁸ Patients must be honest and candid with healthcare providers, and knowing that their private health information is protected by all possible means can help encourage candor. Furthermore, with confidence in the government at an all-time low,²⁵⁹ anything that can be done to lend credibility to and increase the public's confidence in the system should be pursued. Again, states should be encouraged to use all available means to protect patient privacy, particularly when they undertake efforts to collect and maintain private health information. The following Part proposes a solution to the issues relating to law enforcement access to PDMP data that effectively balances the need for law enforcement with patients' privacy interests.

V. BALANCING THE INTERESTS OF EVERYONE: HOW TO GIVE LAW ENFORCEMENT ACCESS TO PDMP DATA WITHOUT VIOLATING PATIENT PRIVACY

Because patients' legitimate expectation of privacy means law enforcement must get a warrant before accessing PDMP data, alternative means may be necessary for law enforcement to effectively combat sophisticated drug diversion operations.²⁶⁰ The need for enforcing drug laws is still an important governmental interest, particularly in light of the rise in prescription drug abuse and overdose deaths.²⁶¹ By simply giving law enforcement unfettered access to de-identified PDMP information about Schedule II drugs (or to specific commonly-abused drugs), states can balance everyone's interests, giving law enforcement an effective tool for investigating crimes and protecting the privacy of patients.

The primary issue with law enforcement access to PDMP data is that the data contains personally identifiable health information, including patients'

²⁵⁶ NAMSDDL, *supra* note 21, at 15.

²⁵⁷ See 5 U.S.C. § 552(b)(1)–(9).

²⁵⁸ See Kam, *supra* note 51.

²⁵⁹ Mollie Reilly, *Congress Approval Rating Drops to Dismal 5 Percent in Poll*, HUFFINGTON POST (Oct. 9, 2013), http://www.huffingtonpost.com/2013/10/09/congress-approval-rating_n_4069899.html.

²⁶⁰ See Dutko, *supra* note 48, at 758–60; see also Kam, *supra* note 51.

²⁶¹ See *supra* Part I.

names, contact information and prescription histories.²⁶² Patients are entitled to assert privacy interests in this type of information; therefore, it should not be the subject of warrantless or unconsented search and disclosure.²⁶³ However, there is no reason an agency like the DEA, which has administrative authority over prescribers and dispensers, could not obtain information about doctors and pharmacists so long as the information does not contain personally identifiable health information about patients.

In this context, the administrative subpoena is appropriate, even for the purpose of criminal prosecution, because of the authority administrative agencies have over doctors and pharmacists. While this type of information may lead to criminal charges, doctors and pharmacists do not have the same privacy interest in the prescriptions they write and fill as patients have in the prescriptions they take.²⁶⁴ Furthermore, an administrative subpoena is not invalid simply because it seeks information as part of a criminal investigation.²⁶⁵ This information could be used to identify doctors that may be complicit in drug diversion rings,²⁶⁶ or doctors that are irresponsibly prescribing drugs.²⁶⁷

Law enforcement could also be given access to PDMP data without a warrant as long as the names of patients and their prescription histories are separated in a way that prevents the names and health information from being correlated. For example, law enforcement could be given access to the names of patients receiving prescriptions, but not the specific prescriptions they received. Also, law enforcement could access lists of the Schedule II prescriptions and their quantities, but not the names of the patients receiving the drugs.²⁶⁸ In this way, law enforcement could examine PDMP data for suspicious activity, such as excessive quantities of drugs going to a single patient or fake names and stolen identities among the names of patients receiving prescription drugs. Furthermore, by restricting this unfettered access to info relating to Schedule II drugs or even just a specific group of Schedule II drugs that are commonly abused, PDMPs can prevent patients from being identified if they take unique combinations of medications tailored to a specific set of conditions that are unique to that individual.

²⁶² See Kam, *supra* note 51.

²⁶³ See *supra* Part IV.A.

²⁶⁴ See *Whalen v. Roe*, 429 U.S. 589, 602 (1977); *Ass'n of Am. Physicians & Surgeons v. Weinberger*, 395 F. Supp. 125, 135–36 (N.D. Ill. 1975).

²⁶⁵ See *United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108, 1116 (9th Cir. 2012).

²⁶⁶ See Robert Lowes, *14 Florida Physicians Indicted in 'Pill Mill' Bust*, MEDSCAPE MED. NEWS (Aug. 30, 2011), <http://www.medscape.com/viewarticle/748811>.

²⁶⁷ See *Painkiller Crackdown*, *supra* note 14.

²⁶⁸ See *Weinberger*, 395 F. Supp. at 135–36. The coding procedures used to ensure confidentiality in this case could be used when law enforcement accesses PDMP data to protect the confidentiality of patients. *Id.* at 136.

Law enforcement could use this type of information to establish the probable cause necessary to get a warrant for the personally identifiable information without violating the privacy rights of innocent patients. De-identified health information is often already reported for regulatory purposes, such as tracking public health trends and ensuring the proper and efficient dispensation of public healthcare funds.²⁶⁹

By giving law enforcement limited access to this type of information, the privacy rights of patients and the need for law enforcement can be effectively balanced. It may require some extra work by law enforcement agencies when investigating patients, but easing the workload of law enforcement is not a justification for invading the privacy of individuals because there is no end to the invasions of privacy such a justification would allow. And, any extra work would likely be minimal under the scheme described above. Because patients have a legitimate expectation of privacy in their personally identifiable PDMP data, the Fourth Amendment requires that law enforcement obtain a warrant before accessing personally identifiable PDMP data. Allowing law enforcement to access de-identified data in a manner described above can quell any concerns by law enforcement, if they fear they won't have sufficient access to these potentially powerful tools for investigating drug crimes, while protecting patient privacy.

VI. CONCLUSION

Prescription drug abuse is an increasingly prevalent problem in the United States with far reaching consequences.²⁷⁰ Prescription Drug Monitoring Programs are an effective and necessary way to prevent and control the diversion and abuse of prescription drugs.²⁷¹ Almost every state has implemented a PDMP,²⁷² and the federal government has stood behind this initiative.²⁷³ Although PDMPs are necessary, their existence presents a potentially significant invasion on patient privacy.²⁷⁴ This invasion of privacy is most egregious when a law enforcement agency, solely for law enforcement purposes, can access PDMP information without first obtaining a warrant. Patients have a legitimate privacy interest in their personal prescription information, as they do in other personal health information, and the need for law enforcement does not, by itself, outweigh this privacy interest.²⁷⁵

²⁶⁹ See *id.*

²⁷⁰ See *supra* Part I.

²⁷¹ See *supra* Part II.B.

²⁷² NAMSDDL, *supra* note 21, at 6.

²⁷³ See BLUMENSCHNEIN ET AL., *supra* note 15, at 3.

²⁷⁴ See *supra* Part II.C.

²⁷⁵ See *supra* Part IV.

In addition to requiring law enforcement to get a warrant, states should be encouraged to include other privacy protections within their PDMPs, and some already do.²⁷⁶ States should specifically exempt PDMP data from public records laws, and create civil and/or criminal penalties for the wrongful access, use, and disclosure of PDMP data. By taking these measures, states can demonstrate a commitment to protecting patient privacy, and likely improve public confidence that private health information will not be disclosed wrongfully. States could also benefit financially, or at least help offset the cost of implementing their PDMPs, by imposing their own penalties, as opposed to federal penalties under the HIPAA Privacy Rule.²⁷⁷ Furthermore, there are commonly used methods to protect patient privacy²⁷⁸ that could allow law enforcement access to some PDMP data without violating this privacy interest. Thus, the privacy interests of patients and the government's interests in enforcing its laws can be effectively balanced.

Therefore, patients have a legitimate expectation of privacy in their personally identifiable PDMP data, and the Fourth Amendment requires that law enforcement obtain a warrant before accessing personally identifiable PDMP data. Our health is one of our most personal and private traits, often outside of our control, embarrassing, or potentially damaging to our reputation.²⁷⁹ To allow the government to invade this privacy without first justifying its intrusion based on a showing of probable cause stands directly against the protections provided by the Fourth Amendment. If government agents cannot search our physical medicine cabinets without getting a warrant, they should not be able to search PDMPs, our virtual medicine cabinets, without doing the same. Our doctors and pharmacists should be the only ones minding our meds, not law enforcement.

*Devon T. Unger**

²⁷⁶ NAMSDL, *supra* note 21, at 36–37.

²⁷⁷ See *supra* Part IV.C.

²⁷⁸ See *Ass'n of Am. Physicians & Surgeons v. Weinberger*, 395 F. Supp. 125, 135 (N.D. Ill. 1975).

²⁷⁹ Complaint in Intervention, *supra* note 61, at 13.

* Senior Notes Editor, *West Virginia Law Review*, Vol. 117; Best Student Note Designation Recipient; J.D. Candidate, West Virginia University College of Law, 2015; B.S. in Journalism, West Virginia University, 2011. The Author would like to thank former *Law Review* editor Justin Kearns for his dedicated assistance during the drafting of this Note; fellow *Law Review* editors Brandon Cole, Francesca Miller, Grace Hurney, and Katherine Moore for their diligent efforts editing and providing valuable feedback; and all the other current and former *Law Review* editors for their hard work making this publication possible. The Author would also like to thank the many professors who, over the course of his academic career, have inspired the passion that made this Note possible. Finally, the Author would like to thank his family, and especially his wife, Samantha Marie Unger, and his parents Thomas and Susan Unger, for all of their love and support throughout his life. Any errors contained herein are my own.

