JOURNAL OF HEALTH CARE FINANCE

Summer 2019

Do Prescription Drug Monitoring Programs Compromise Patient Privacy By Remaining Outside Federal and Most States' Privacy Standards?

Colleen Paddon Simek, JD, LLM

INTRODUCTION

As the United States gradually adopted a more liberal treatment of patient pain symptoms, a very serious crises began to emerge.[1] The opioid epidemic is not only creating a population dependent on prescription drugs, but it is costing lives.[2] Prescription Drug Monitoring Programs, created to better surveil and protect the public, track the prescribing and dispensing patterns of certain types of prescription drugs classified as "controlled substances."[3] In doing so, Prescription Drug Monitoring Programs ("PDMPs") store personally identifiable medical information within state electronic databases, some of which would be considered highly sensitive in nature.[4] Storage of this information allows pharmacies and prescribers to monitor what prescription drugs are being dispensed to patients, and in what quantity and frequency.[5] Each state's PDMP law varies by type of identifying information captured in the database, and who may have access to the database.[6] Generally speaking, personally identifiable health and medical information in the United States is afforded certain federal protections, as entities who store such information are governed by a federal regulation known as the Health Insurance Portability and Accountability Act. Similarly, some states have created their own privacy laws to address privacy protections of personal information. Unfortunately, however, PDMPs do not fall within federal or state privacy protection laws. Thus, PDMPs are not required to comport with privacy and security protections over the personal health and medical information that is stored in the database. This has caused both patients and providers alike to challenge the constitutionality and legality of the databases.[7]

Below I will first describe the history and background of PDMPs, including how they developed and what they function like today. Then, I will discuss the constitutional challenges that have been made against PDMPs, including cases that illustrate individual privacy concerns regarding prescription drug and medical information, and whether courts have allowed third parties such as law enforcement agencies to access state PDMPs. I will also discuss the compelling interest of the states when it comes to protecting and promoting the general health and welfare of the population though the use of PDMPs. Lastly, I will demonstrate that in order to effect a reasonable balance and reduce the variability between state PDMP laws, action from the federal government is required. The federal government should require PDMPs to comply with a national, standardized law that continues to emphasize the public health purpose of PDMPs, but also requires each state to conform to a national privacy standard. I firmly recommend that state managed PDMP databases should be treated as "covered entities" under the Health Insurance Portability and Accountability Act, in order to provide a baseline for direction and regulation over state PDMPs. In doing so, both privacy and security protections will be afforded to individuals whose information is captured by PDMP databases.

---

[1] Rebecca Haffajee, *Preventing Opioid Misuse with Prescription Drug Monitoring Programs: A Framework for Evaluating the Success of State Public Health Laws*, 67 HASTINGS L.J. 1621, 1624 (2016).

[2] Centers for Disease Control and Prevention: *Opioid Overdose and Drug Overdose Deaths*, [hereinafter "CDC Drug Overdose Deaths"] https://www.cdc.gov/drugoverdose/data/statedeaths.html (last visited: July 13, 2019).

[3] 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. 345 (2014).

[4] *Id.* at 347.

[5] *Id.* at 347-348.

[6] *Id.* at 349-350.

[7] Stephen P. Wood, *Prescription Monitoring Programs: HIPAA, Cybersecurity and Privacy, Harvard Law Bill of Health: Examining the Intersection of Health Law, Biotechnology, and Bioethics*, June 17, 2018, http://blog.petrieflom.law.harvard.edu/2018/06/17/prescription-monitoring-programs-hippa-cyber-security-and-privacy/ (last visited July 2, 2019).

I. The Opioid Crisis and Misuse of Prescription Drugs

A. Not a New Epidemic

On October 26, 2017, President Trump announced the opioid crisis to be a national Public Health Emergency under federal law.[8] The opioid crisis the United States currently faces, however, is not a *new* epidemic. The crisis emerged as a result of many different events and influences. It began gradually at first, dating back to the 1970s when The American Pain Society was formed in order to increase public awareness of pain management and research.[9] Even today, its vision remains to imagine "a world where pain prevention and relief are available to all people."[10] Later, during the 1980s, a privately held pharmaceutical company called Purdue Pharma released a new painkiller drug to the market called "MS Contin," a morphine pill with an ability to control the release of its effects because the drug slowly dissolved into the bloodstream over many hours.[11] In the late 1980s, the patent for MS Contin expired and Purdue Pharma was on the search for another drug to take its place in the marketplace.[12] Simultaneously, starting in the early 1990s, the medical field entered a new era where there was a "heightened focus on pain management."[13] The American Society for Pain Management Nursing ("ASPMN") emerged in the early 1990s with the hope of providing a network for nurses working in pain management, with the goal of promoting optimal nursing care for people affected by pain.[14] Finally, in 1995, Purdue Pharma had developed their replacement for the drug MS Contin, the new prescription painkiller OxyContin was released.[15] The American Pain Society then began to promote a new slogan, "Pain: The Fifth Vital Sign," which led physicians to believe they should be treating pain as routinely as they do the other vital signs, which are objective and not subjective in nature (pulse, blood pressure, body temperature, and respiration).[16] In fact, the Federation of State Medical Boards passed a policy in 2004 that encouraged state medical boards to "consider under-treatment of pain an equally serious violation of the standard of care as over-treatment."[17] The Joint Commission for Accreditation of Healthcare Organizations ("JCAHO") has adopted a similar policy.[18] This caused hospitals to be assessed and accredited based on how physicians attended to a patient's complaint of pain.[19] It was with this heightened focus on pain management, that physicians

[8] The White House, *Ending America's Opioid Crisis* (2019), www.whitehouse.gov/opioids (last visited June 26, 2019).
[9] The American Pain Society: *History of the American Pain Society*, http://americanpainsociety.org/about-us/history/overview (last visited July 2, 2019).
[10] The American Pain Society: *Mission, Vision, and Values*, http://americanpainsociety.org/about-us/overview (last visited July 2, 2019).
[11] Patrick Radden Keefe, *The Family That Built an Empire of Pain*, The New Yorker, October 30, 2017, https://www.newyorker.com/magazine/2017/10/30/the-family-that-built-an-empire-of-pain (last visited June 26, 2019).
[12] *Id.*
[13] Haffajee, *supra* note 1 at 1624.
[14] American Society for Pain Management Nursing: *Mission*, http://www.aspmn.org/Pages/default.aspx (last visited June 26, 2019).
[15] Keefe, *supra* note 11.
[16] Sam Quinones, *Dreamland: The True Tale of America's Opiate Epidemic*, 95 (2015).
[17] Haffajee, *supra* note 1 at 1628.
[18] Quinones, *supra* note 16 at 95.
[19] *Id.*

became more liberal in their prescribing methods.[20] Immediately following the release of OxyContin, Purdue Pharma marketed the drug as a pill that is less addictive, less subject to abuse and less likely to cause withdrawal symptoms than other pain medications.[21] Ironically, OxyContin's only active ingredient is oxycodone, which is a "chemical cousin of heroin," twice as powerful as morphine.[22] The argument that it was a non-addictive prescription pain pill originated from Purdue Pharma; they claimed that since it was a timed-release drug, that patients were less likely to develop dependence on the medication.[23] Purdue Pharma often gave OxyContin coupons to physicians who could gift them to patients as a "onetime free prescription" at certain participating pharmacies.[24] Very recently, it is reported that almost every state in the United States has filed a lawsuit against Purdue Pharma, alleging that it downplayed the risks associated with addiction to OxyContin.[25]

B. A Population of Addicts

This massive marketing of painkillers, including OxyContin, slowly turned the United States population into addicts; prescription opioid misuse in the United States has now risen to an epidemic proportion.[26] An article from 2013 revealed that drug overdoses actually kill more people than automobile accidents do – at least that was the case in twenty nine states.[27] In fact, out of the total number of drug overdoses in 2013, illicit drugs were not actually the primary cause; over half of the deaths were instead associated with prescription drugs.[28] The rate of overdose deaths increased by over nine percent between the years 2016 and 2017.[29] This has resulted in more than forty seven thousand deaths in the United States during 2017 due to drug overdose involving opioids.[30] It was this over prescribing and misuse of prescription drugs that led to "doctor shopping" and "pill mills." Doctor shopping is the practice by which patients attempt to obtain prescriptions from multiple different providers in an effort to obtain more prescription drugs than they should be normally taking.[31] Prescription drug abusers are able to seek out large quantities of drugs with frequent refills, and in most cases the doctors are not aware that their

---

[20] Haffajee, *supra* note 1 at 1624.
[21] Quinones, *supra* note 16 at 264.
[22] Keefe, *supra* note 11.
[23] Quinones, *supra* note 16 at 132.
[24] *Id*. at 134.
[25] Berkeley Lovelace, *Nearly Every U.S. State Is Now Suing OxyContin Maker Purdue Pharma*, June 6, 2019, https://www.cnbc.com/2019/06/04/nearly-every-us-state-is-now-suing-oxycontin-maker-purdue-pharma.html (last visited: June 26, 2019).
[26] Haffajee, *supra* note 1 at 1629.
[27] Reid Wilson, *Drug Overdoses Kill More People Than Auto Accidents in 29 States*, The Washington Post, October 8, 2013, https://www.washingtonpost.com/blogs/govbeat/wp/2013/10/08/drug-overdoses-kill-more-people-than-auto-accidents-in-29-states/?utm_term=.c939ec0222ff (last visited June 26, 2019).
[28] Emma Masse, *Missouri Shows the True Meaning of the "Show-Me" State - Missouri's Unfounded Hesitation to Enact a Prescription Drug Monitoring Program*, 83 MO. L. REV. 217 (2018).
[29] CDC Drug Overdose Deaths, *supra* note 2.
[30] U.S. Dept. of Health & Human Services, Office of Inspector General: *Oversight of Opioid Prescribing and Monitoring of Opioid Use: States Have Taken Action to Address the Opioid Epidemic* (July 2019), [hereinafter "HHS OIG Oversight of Opioid Prescribing"] https://oig.hhs.gov/oas/reports/region9/91801005.pdf (last visited July 30, 2019).
[31] John Butler, William Becker & Keith Humphreys, *Law and the Opioid Crisis: An Inter-Disciplinary Examination: Big Data and the Opioid Crisis: Balancing Patient Privacy with Public Health*, 46 J.L. MED. & ETHICS 440, 441 (2018).

patients are getting prescriptions from multiple different sources.[32] Pill mills, on the other hand, involve the illegal sale of prescription drugs out of physician-run pain clinics.[33] Since licensed physicians may purchase opioids in bulk, they are able to re-package them and sell them to patients for up to three hundred percent of the fair market value that they would get from third-party payors.[34] While clearly this practice is illegal, it is extremely profitable for these rogue physicians to dispense directly to patients, after only a very brief medical evaluation.[35] Some of the largest and most profitable pill mill clinics are located in the state of Florida, where they attract drug seeking patients because there is a promise of on-site drug dispensing.[36]

II. State and Federal Government Response to the Opioid Crisis

A. The Controlled Substances Act

In an effort to prevent misuse of controlled substances, the federal government, through the United States Congress, enacted the Controlled Substances Act in 1970 when it found that the "improper use of controlled substances have a substantial and detrimental effect on the health and general welfare of the American people."[37] The Controlled Substances Act ("CSA") makes it unlawful to manufacture, distribute, dispense, or possess any controlled substances, except as permitted by the Act.[38] The CSA effectively placed regulatory controls over various prescription medications with the Drug and Enforcement Agency ("DEA").[39] Under the CSA, it is illegal to prescribe or dispense certain prescription medications without first registering with the DEA Administrator.[40] Congress classifies these prescription medications into five categories of controlled substances called "Schedules," each Schedule is based on the drug's accepted medical uses, the potential for abuse, and the likelihood of psychological or physical dependency.[41] For example, Schedule I controlled substances are those that have "no currently accepted medical use for treatment in the United States,"[42] these include opiates such as heroin and mescaline.[43] Schedule II controlled substances have "currently accepted medical use for treatment in the United States," but have severe restrictions.[44] Schedule II controlled substances include combination drugs such as Vicodin, OxyContin, fentanyl and Ritalin.[45] Many of the drugs that fall within Schedule II may sound familiar to you, as they are used to treat common conditions like ADHD or severe and chronic pain. Schedule III controlled substances have a moderate to low potential

---

[32] Joanna Shepherd, *Combating the Prescription Painkiller Epidemic: A National Prescription Drug Reporting Program*, 40 AM. J.L. AND MED. 85, 92 (2014).
[33] Ashley Dutko, *Florida's Fight Against Prescription Drug Abuse: Prescription Drug Monitoring Program*, 34 NOVA L. REV. 739, 743 (2010).
[34] Shepherd, *supra* note 32 at 96.
[35] *Id.*
[36] Dutko, *supra* note 33 at 745.
[37] 21 U.S.C.S. § 801.
[38] *Id.* § 841.
[39] Shepherd, *supra* note 32 at 102-103.
[40] *Id.*
[41] 21 U.S.C.S. § 812.
[42] *Id.*
[43] U.S. Drug Enforcement Administration, *Drug Scheduling* [hereinafter "DEA Scheduling"] (2019), https://www.dea.gov/drug-scheduling (last visited June 26, 2019).
[44] 21 U.S.C.S. § 812.
[45] DEA Scheduling, *supra* note 43.

for dependence and all currently have accepted medical uses in treatment in the United States.[46] Schedule III drugs include Tylenol with codeine, anabolic steroids and testosterone.[47] Schedule IV controlled substances are defined as drugs with "a low potential for abuse" and have a "currently accepted medical use for treatment in the United States."[48] Schedule IV drugs include Valium, Xanax, Darvocet, Ativan, and Tramadol.[49] Lastly, Schedule V controlled substances have "a low potential for abuse" and have acceptable medical uses for treatment.[50] Schedule V drugs include Robitussin and Lyrica.[51] Robitussin is available over the counter at your local pharmacy. Some of the controlled substances listed above or included in the Schedules of controlled substances, however, are prescribed to treat mental health or substance abuse disorders. Additionally, testosterone, a Schedule III drug, can be used to treat gender identity disorders, sexual dysfunction disorders, and HIV and AIDS.[52] Prescriptions delivered to patients by their physicians for these purposes are clearly more sensitive in nature than that of an over-the-counter drug such as Robitussin.

B. State Prescription Drug Monitoring Programs

In order to regulate the use of controlled substances and reduce the risk of addiction or other misuse, states responded by implementing Prescription Drug Monitoring Programs ("PDMPs").[53] The Federal Government provides financial support to states that wish to enact and implement statewide PDMPs.[54] New York was the first state to implement its own state run PDMP in 1918.[55] California was another early state that adopted its own PDMP program in 1939.[56] Currently, all states have some version of a PDMP, with Missouri being the last state to implement its PDMP in 2017.[57] The Center for Disease Control ("CDC") describes PDMPs "as among the most promising state level intervention to improve opioid prescribing, inform clinical practice and protect patients at risk."[58] PDMPs, as we know them today, are statewide electronic databases that collect and store information regarding what prescription drugs are both prescribed and dispensed to patients within a given state.[59] PDMPs generally monitor and track prescriptions that are included within Schedules II through V of the controlled substance Schedules.[60] Oregon law, however, requires PDMP reporting only when the prescription drug is classified within Schedules

---

[46] 21 U.S.C.S. § 812.
[47] DEA Scheduling, *supra* note 43.
[48] 21 U.S.C.S. § 812.
[49] DEA Scheduling, *supra* note 43.
[50] 21 U.S.C.S. § 812.
[51] DEA Scheduling, *supra* note 43.
[52] Katherine Margo & Robert Winn, *Testosterone Treatments: Why, When, and How?*, 73 AM. ACADEMY OF FAMILY PHYSICIANS, 9, 1593 (2006).
[53] Unger, *supra* note 3 at 347-348.
[54] Masse, *supra* note 28 at 218.
[55] Alliance of States with Prescription Monitoring Programs, *Prescription Monitoring Programs* 5 (Oct. 18, 2010), http://www.pdmpassist.org/pdf/PPTs/LI2010/1-PMP-Overview-History.pdf (last visited June 26, 2019).
[56] 16 C.C.R. § 1715.5.
[57] Beth Schwartzapfel, *Guess Who's Tracking Your Prescription Drugs? Your Doctor, your pharmacist…and the Police*. The Marshall Project, August 2, 2017, https://www.themarshallproject.org/2017/08/02/guess-whos-tracking-your-prescription-drugs (last visited June 26, 2019).
[58] Centers for Disease Control and Prevention, *What States Need to Know about PDMPs* (2019), [hereinafter "CDC State PDMPs"] www.cdc.gov/drugoverdose/pdmp/states.html (last visited June 26, 2019).
[59] Unger, *supra* note 3 at 345.
[60] Haffajee, *supra* note 1 at 1636.

II through IV.[61] Thirty five states, in total, require PDMP reporting when the prescription drug is classified in Schedules II through V.[62] Recall that Schedule V prescriptions have the lowest potential for abuse and addiction, and include drugs that are common for ailments such as coughing or diarrhea.[63] PDMPs "hold the potential to both facilitate legitimate prescribing of controlled substances, and also mitigate prescription drug misuse."[64] This is accomplished because the PDMP system assists physicians in understanding what prescriptions their patients have been filling, how often they are being filled, and in what quantity.[65] As a result, the state's PDMP aids in decreasing prescription drug abuse to prevent doctors from unknowingly prescribing certain drugs to a potential addict, who may be searching for unnecessary quantities of prescription drugs, also known as "doctor shopping."[66] The PDMP serves as a tool to help identify when patients may be showing signs of prescription drug abuse.[67] The ultimate goal of PDMPs is thus to improve individual and population level health, in light of the oversupply of opioids discussed in Section I.[68] PDMPs also allow providers and physicians to address issues related to risks that can occur with prescribing certain pills in combination with others, and address problems related to side effects.[69]

The scope of information contained in the database varies state by state. The information reported to and stored in the database typically includes, but is not necessarily limited to: name, address, date of birth, drug history, including drug name, prescriber and pharmacy dispenser.[70] For example, Oregon law requires its state pharmacies to report to the PDMP, within seventy-two hours of a prescription fill or refill, specific information to the Oregon Health Authority, including: the name, address, phone number, date of birth and sex of the patient for whom the prescription drug was prescribed; along with: pharmacy name, prescribing doctor's name, date of prescription, national drug code number, prescription number, quantity of the prescription drug dispensed, number of days for which the prescription drug was dispensed, and the number of refills that was authorized by the prescribing physician.[71] While the obligation to report to the database lies with the pharmacy as dispenser of the prescription drugs, there are various other individuals that have access to the PDMP itself. California, for example, has a state run PDMP called "CURES," which stands for the Controlled Substance Utilization Review and Evaluation System.[72] To gain access to California's CURES, one must first be a registered user of the program.[73] Registration for the program is not limited to the dispensing pharmacy that reports the information, other permissible registered users include: dentists, physicians, optometrists, physician assistants, podiatrists, nurse

---

[61] Or. Rev. Stat. § 431A.860.
[62] Prescription Monitoring Program Training and Technical Assistance Center, *PDMP Frequently Asked Questions*, http://www.pdmpassist.org/content/prescription-drug-monitoring-frequently-asked-questions-faq (last visited July 2, 2019).
[63] Masse, *supra* note 28 at 220-221.
[64] Haffajee, *supra* note 1 at 1637.
[65] Masse, *supra* note 28 at 218.
[66] *Id.*
[67] Wood, *supra* note 7.
[68] Haffajee, *supra* note 1 at 1635.
[69] Jesse C Vivian, *Privacy and Prescription Drug Monitoring Programs*, 39(5) U.S. PHARM. 44-46 (2014).
[70] *See e.g.* Fla. Stat. § 893.055.
[71] Or. Rev. Stat. § 431A.860.
[72] Cal. Health & Safety Code § 11165.1.
[73] Cassandra Rivais & Bruce White, *The Opioid Epidemic is Not New: Time to Change the Practice of Medicine*, 11 ALB. GOV'T L. REV. 58, 60-61 (2017-2018).

midwives, nurse practitioners and veterinarians.[74] California's CURES also allows law enforcement officers to use the database to monitor prescribing activities.[75] In fact, starting in 2009, CURES was modified to allow pre-registered users, including law enforcement, to gain access to records in a more efficient manner through an electronic real-time system without having to request information via telephone or facsimile.[76]

PDMPs contain a wide scope of information, and there are many different users that are able to obtain access to the system for various purposes. Reasonable minds would assume that PDMPs would have in place certain privacy or security protocols to assure that no unauthorized individuals are able to access, use, or disclose information without a direct need-to-know. In the forthcoming sections, I will demonstrate that even though certain states have attempted to address privacy issues within their PDMP laws,[77] PDMP systems are falling between the cracks of privacy protections. As a result, one major fundamental challenge that PDMPs face is from individual claims asserting privacy rights violations grounded in the Fourth and Fourteenth Amendments, along with arguments made relating to violations of state or federal confidentiality laws.[78] In the case examples that follow, both patients and prescribers have raised relevant privacy concerns.[79]

III. Constitutional Challenges to PDMPs

A. *Whalen v. Roe* and the Balancing Test

Before I delve into the obvious lack of privacy and security standards within PDMPs, it is first necessary to cover one of the most important landmark cases that questioned the overall constitutionality of PDMPs from an information privacy perspective.[80] In the 1977 case of *Whalen v. Roe,* patients and doctors who receive and prescribe Schedule II drugs brought an action in the U.S. District Court days before New York's PDMP law requiring patient identification became effective.[81] Prior to this new law, the New York Legislature recognized its state PDMP was not adequately serving a useful purpose.[82] In response to this concern, under the new law, doctors who prescribe Schedule II drugs to their patients must prepare a form that identifies the prescribing physician, the dispensing pharmacy, the drug and dosage, and also the name, address and age of the patient.[83] The new law requires one copy of the form to be kept by the physician, one to be given to the pharmacist, and the last copy to be forwarded to the New York State Department of Health.[84] During the case, the court discovered that approximately one hundred thousand Schedule II prescription forms were being processed by the Department of Health on a monthly basis.[85] Once there, the forms were sorted, coded and logged, and eventually the data was placed on magnetic tapes for computer processing.[86] Thus, under the new law, patients were individually

[74] *Id.*
[75] *Id.*
[76] *Id.* at 58.
[77] *See e.g.* Cal. Health & Safety Code § 11165(c)(1).
[78] Haffajee, *supra* note 1 at 1656.
[79] *Id.*
[80] *Whalen v. Roe*, 429 U.S. 589 (1977).
[81] *Id.* at 595.
[82] *Id.* at 592.
[83] *Id.* at 593.
[84] *Id.*
[85] *Id.* at 592.
[86] *Id.* at 593.

identified, along with their prescription drug information, and were recorded and stored in an electronic database.[87] At the electronic processing facility, there were seventeen employees with access to the files, and twenty four investigators that had authority to search cases in which there was a suspected over dispensing.[88] The plaintiffs in this case argued that the patient identification aspect of the law was unconstitutional because it violated and invaded individual privacy rights.[89] They also argued that the requirement for patient identification could deter individuals from seeking treatment because potential patients may fear that misuse of the computerized data would cause them to be stigmatized as a "drug addict."[90] The three judge panel at the U.S. District Court level held that the state of New York was "unable to demonstrate the necessity for the patient-identification requirement…" and held the New York statute "unconstitutional as an unreasonable, unnecessary and arbitrary interference with the right of the individual to his personal liberty…"[91] On appeal, however, the U.S. Supreme Court reversed the District Court's decision for a variety of reasons.[92] Namely, the Supreme Court opined that the patient identification requirement was not "an invasion of any right or liberty protected by the Fourteenth Amendment" and the statute was a "reasonable exercise of the state's police power," and thus did not impair any individual privacy interests.[93]

Whalen illustrates that an individual's privacy rights are not violated in cases where a state requires electronic recording of all patients who obtain and fill prescriptions for certain Schedules of drugs under the CSA.[94] The case suggests that the right to privacy of one's prescription drug records must be weighed against important competing interests; in *Whalen,* it was the state's interest in monitoring the use of addictive prescription drugs.[95] It is important to note that the Fourth Amendment was not discussed or argued in this case, however, *Whalen* set the stage for a series of subsequent cases whereby plaintiffs exercised their right to file a civil action under federal law for deprivation of rights, asserting violations of the Fourth Amendment of the U.S. Constitution. [96] In each case, the plaintiffs allege their fundamental right to privacy of their prescription drug records or medical records had been violated. The Fourth Amendment guarantees citizens the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[97] The Supreme Court has recognized that this protection extends to the protection of individual people, and includes the "individual interest in avoiding disclosure of personal matters, and the interest in independence when making certain kinds of important decisions."[98] That being said, following an application of *Whalen's* "balancing test" in each case discussed below, most courts struggle to reach a conclusion that weighs in favor of a plaintiff's claim regarding violation of their privacy rights.

---

[87] *Id.*
[88] *Id.* at 594.
[89] *Id.* at 592.
[90] *Id. at* 595.
[91] *Id.* at 596.
[92] *Id. at* 599.
[93] *Id. at* 604.
[94] *Id.*
[95] *Doe v. Southeastern Pa. Transp. Auth*., 72 F.3d 1133, 1138 (3d Cir. 1995).
[96] 42 U.S.C.S. § 1983.
[97] U.S. Const. amend. IV.
[98] *Whalen,* 429 U.S. at 599-600.

B. Fourth Amendment Challenges

In the 1995 case of *Doe v. Southeastern Pennsylvania Transportation Authority*, employee John Doe was HIV-positive.[99] In an effort to keep his diagnosis confidential from his co-workers, he asked his supervisor if anyone reviewed employee names in association with what drugs they might be taking.[100] Doe's supervisor assured him that the only instance in which the Southeastern Pennsylvania Transportation Authority (SEPTA) would investigate an employee's prescription use is in cases where there was suspected narcotics abuse.[101] In reliance on these assurances, Doe filled his prescription for Retrovir, a drug used solely to treat HIV.[102] Thereafter, SEPTA switched to Rite-Aid Pharmacy to be the sole provider for all of its employee's prescription drug fulfillment needs.[103] Following this change, Doe was not informed of any changes to the company's policies, including its policy on privacy of prescription drug records.[104] As part of her main duty to lower self-insured health care costs at SEPTA, the Chief Administrative Officer requested and received utilization reports from Rite-Aid.[105] These reports included a line-by-line description of each employee's prescription drug utilizations, including: the name of each employee, the prescribing doctor, the dispense date, the name of the drug, and the number of days supplied.[106] Following a review of this list, the CAO was able to reach the obvious conclusion that Doe was HIV-positive.[107] Once Doe discovered this, he brought an action against the CAO (in her individual and official capacity) and also against his employer, SEPTA, alleging they violated his right to privacy when his HIV status was disclosed to the CAO and other senior level individuals in the SEPTA office as a result of the CAO's search of his prescription drug records.[108] Citing *Whalen*, the Court of Appeals in *Doe* recognized that individuals have a right to privacy in their medical records,[109] however, this right is not absolute.[110] "As with many individual rights, the right of privacy in one's prescription drug records must be balanced against important competing interests."[111] Ultimately the court found that SEPTA's need to access employee prescription records under its self-insured health insurance plan outweighed Doe's interest in keeping his prescription drug purchases confidential because the utilization report was disclosed to SEPTA's CAO only for the purpose of monitoring the use and costs of the plan.[112]

Although the court was unwilling to find a privacy violation in *Doe*, a 2001 case where a state hospital implemented a policy that required all pregnant women be subjected to a mandatory urine drug screening was decided as unconstitutional.[113] In *Ferguson v. City of Charleston*, hospital staff members were required to test all pregnant patients in order to detect drug abuse;

---

[99] *Doe*, 72 F.3d at 1134.
[100] *Id.*
[101] *Id.* at 1135.
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.* at 1135-1136.
[106] *Id.* at 1135.
[107] *Id.* at 1136.
[108] *Id.* at 1137.
[109] *Id.*
[110] *Id.* at 1138.
[111] *Id.*
[112] *Id.* at 1143.
[113] *Ferguson v. City of Charleston*, 532 U.S. 67, 69 (2001).

positive results of such tests were then reported to the police.[114] The United States Supreme Court found that the hospital's policy of urine testing was not only an unreasonable search and seizure in violation of the Fourth Amendment, but also the testing was done without prior consent by the patients.[115] In applying *Whalen's* balancing test, the "interest in using the threat of criminal sanctions to deter drug use could not justify a departure from the general rule that an official nonconsensual search is unconstitutional."[116] This case is easily distinguishable because the ultimate goal of the policy did not justify a nonconsensual invasion into each patients' medical records. In this case, there was no prior warrant obtained, no probable cause or reasonable suspicion to conduct the search, and no knowledge of, or prior verbal or written consent.[117] As I will further discuss in Section V below, individuals have a reasonable expectation of privacy of their medical records, and this expectation is supported by judicial precedent which dictates that there is a recognized heightened expectation of privacy for medical information.[118] The *Ferguson* court found exactly that – the court held there is a "reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital…" and that "the results of those tests will not be shared with non-medical personnel without consent."[119]

Although the *Ferguson* court found there was a privacy violation, the 2005 case of *Douglas v. Dobbs* returned to the *Whalen* school of thought when the U.S. Court of Appeals for the Tenth Circuit found in favor of the district attorney's office, despite the fact that it authorized and conducted a search of Douglas' pharmacy prescription drug records.[120] The appellate court noted that Douglas had a constitutional right to privacy in her prescription drug records, however, the search in this case was executed pursuant to a prior court order.[121] In this particular case, Douglas' physician provided information to the police that supported his suspicion that Douglas was obtaining excess prescription drugs by illegally forging prescriptions and also by using an alias.[122] Thus, a court had approved a motion to allow the district attorney's office to conduct a search of Douglas' prescription records found in the state PDMP.[123] In reference to *Whalen's* balancing test, the court noted that it "created a right to privacy in certain personal information, and this includes prescription drug records."[124] However, this right to privacy was not violated in this case, and the district attorney was entitled to qualified immunity.[125]

Douglas illustrates the heart of the "balancing test" contained in the *Whalen* decision. "While individuals have a legitimate expectation of privacy in their prescription purchases of controlled substances, such right must be weighed against the state's interests in monitoring the use of dangerously addictive drugs."[126] Similar to that of *Douglas,* the court found that there was no violation of a plaintiffs right to privacy when a blood test was performed at a hospital upon request by law enforcement in order to determine blood alcohol concentration.[127] In the 2010 case

---

[114] *Id.*
[115] *Id.* at 84.
[116] *Id.* at 69.
[117] *Id.* at 84.
[118] *United States v. Westinghouse Elec. Corp*., 638 F.2d 570, 577 (1980).
[119] *Ferguson,* 532 U.S. at 78.
[120] *Douglas v. Dobbs*, 419 F.3d 1097, 1099 (10th Cir. 2005).
[121] *Id.* at 1102.
[122] *Id.* at 1099.
[123] *Id.* at 1100.
[124] *Id.* at 1101.
[125] *Id.* at 1103.
[126] *Doe,* 72 F.3d at 1143 citing *Whalen,* 429 U.S. at 602.
[127] *State v. Davis,* 161 N.H. 292, 298 (2010).

of *State v. Davis*, a high school student was taken by ambulance to the hospital following a car accident after the student accidentally backed into a tree.[128] While at the hospital, his blood was drawn and tested to determine blood alcohol concentration levels.[129] Thereafter, the student was charged with unlawful possession of alcohol and driving while intoxicated.[130] Pursuant to an investigation into the incident, the police department filed a request for the hospital blood records, and the hospital turned over such records.[131] The student filed a motion to suppress the records alleging that it was a violation of his right to privacy of his medical records. The court noted that the initial blood draw was taken for medical purposes and not for law enforcement purposes.[132] Therefore, the treatment was consensual at that point in time, and the results were requested by law enforcement in connection with an incident giving rise to an investigation, thus there was no violation of the student's right to privacy.[133]

As you may have observed, Fourth Amendment right to privacy actions brought under the federal law's deprivation of rights statute have not typically been successful. In all but one case that was discussed in this section, courts were unwilling to find there was a violation of an individual's right to privacy, either in his or her prescription records or medical records. I believe these findings relate directly back to the *Whalen* court, whereby the U.S. Supreme Court set the precedent for future right to privacy cases. *Whalen* recognized a right to privacy in preventing disclosure by the government of personal matters, however, any legitimate expectations of privacy of one's prescription [or medical] records must be balanced (or weighed) against a state's interest in monitoring the use of dangerously addictive drugs.[134]

IV. Public Health Surveillance

As seen in the cases discussed in Section III, most plaintiffs in the realm of prescription drug and medical record privacy have unsuccessfully argued that their right to privacy was violated based on a balancing of interests between the individual and the state. Generally speaking, states have an interest in protecting and promoting its population's health and well-being.[135] In doing so, a state may exercise its "police power," meaning, its inherent authority to enact laws and regulations in order to "protect, preserve, and promote the health, safety, morals and general welfare of its people."[136] Therefore, each state has an interest in monitoring adverse health conditions, including their causes, trends, and risk factors that affect the population.[137] This is more broadly understood today as "public health surveillance," which often emerges in response to major threats against the public's health.[138] Public health surveillance is necessary to understand hazards in the community.[139] Historically, public health surveillance efforts were geared toward

---

[128] *Id.* at 294-295.
[129] *Id.* at 294.
[130] *Id.*
[131] *Id.*
[132] *Id.* at 298.
[133] *Id.*
[134] *Whalen*, 429 U.S. at 598.
[135] Lawrence O. Gostin & Lindsay F. Wiley, *Public Health Law: Power, Duty, Restraint*, 89 (3rd ed. 2016).
[136] *Id.* at 87-88.
[137] *Id.* at 397-398.
[138] Leo Beletsky, *Deploying Prescription Drug Monitoring To Address the Overdose Crisis: Ideology Meets Reality*, 15 IND. HEALTH L. REV. 139, 148 (2018).
[139] *Id.* at 147- 148.

communicable diseases such as yellow fever.[140] Today, however, there is a much different and much larger crisis the United States is facing – the opioid epidemic.[141]

As discussed in Section II, states began implementing PDMPs in order to improve individual and population level health, in light of the increased abuse of prescription drugs.[142] There are many adverse health consequences that result from prescription drug misuse, such as overdose deaths, emergency room visits, and inpatient admissions, all of which have dramatically increased in correlation with the opioid crisis.[143] Therefore, each state has an interest in monitoring and tracking individual level prescription drug use and their ongoing prescription refills, when it is aimed at identifying possible cases of drug abuse and misuse.[144] PDMPs help to "understand the prevalence and incidence of use of certain drugs, track unexpected or adverse events, and target resources and interventions to patients and geographical areas most in need."[145] Throughout history, however, public health surveillance efforts have created privacy concerns.[146]

It is said that the *Whalen* court "demarcated the limits of privacy based objectives to government surveillance in modern jurisprudence."[147] Clearly, it has been well established by case law that states may make intrusions into individual rights in order to further a legitimate interest, such as monitoring and tracking prescription drug use within a state-run PDMP.[148] Courts have accepted this because states are using their police powers in order "to protect the health, safety, welfare and morals of the community."[149] As a reminder, however, PDMPs contain highly sensitive information, including a patients name, address, date of birth, prescription drug history, quantity dispensed and prescribing physician.[150] Many different types of users may access this system, and in California, its CURES system permits law enforcement officers to search the database to monitor individual prescribing activities.[151] While states may have a legitimate interest in protecting the community, I plan to demonstrate that PDMPs present serious privacy concerns because they lack state or federal regulatory oversight and control. If PDMPs were forced to answer to one federal baseline rule for protection of personally identifiable health information stored in the database, PDMP entities would be incentivized to ensure that privacy and security controls are in place, such that no unauthorized third parties gain access to the data either purposefully or inadvertently.

V. Individual Privacy Rights

A. Reasonable Expectation of Privacy

While there is no express right to privacy contained in the United States Constitution, courts have generally accepted the notion that individuals enjoy a fundamental human right to

[140] *Id.* at 148.
[141] The White House, *supra* note 8.
[142] Haffajee, *supra* note 1 at 1635.
[143] *Id.* at 1630.
[144] Beletsky, *supra* note 138 at 151.
[145] *Id.* at 165.
[146] *Id.* at 149.
[147] *Id.* at 152.
[148] Unger, *supra* note 3 at 356.
[149] Gostin, *supra* note 135 at 77.
[150] *See e.g.* Fla. Stat. § 893.055.
[151] Rivais, *supra* note 73 at 60-61.

privacy.[152] The first official privacy law enacted in the United States was the Federal Privacy Act of 1974.[153] When Congress enacted the Privacy Act, it found that "the privacy of an individual is directly affected by the collection, maintenance, use and dissemination of personal information…"[154] The Privacy Act was essentially shaped by the Health, Education and Welfare Advisory Committee's "Fair Information Practices," which were released in 1973.[155] The Code of Fair Information Practices is based upon five core principles: (1) there may be no data record-keeping systems that are unknown to others, (2) there must be a way for individuals to know what information is being stored about them and how it is being used, (3) there must be a way for an individual to prevent collected information from being used for another non-consensual purpose, (4) individuals must be able to amend or correct their record of information, and (5) organizations storing data must take precautions to prevent unauthorized use of data.[156] Eventually these principles and the Privacy Act transformed into our current federal privacy law, what we now know today as the Health Insurance Portability and Accountability Act, which was originally enacted in 1996. This will be more thoroughly discussed in Section VII below.

First, there is importance in revisiting the historical context of privacy law in the United States in order to understand the impact it has had on privacy as we know it to be today. As previously mentioned, it is a well-established concept that individuals are able to enjoy a fundamental right to privacy of their information. One of the most pivotal cases grounded in criminal law that explored this concept actually dates prior to the Health, Education and Welfare's Fair Information Practices. In *Katz v. United States*, Mr. Katz was convicted of interstate gambling, a federal crime for which he used public telephone booths to further his illegal activities.[157] In order to collect evidence to build a case against Mr. Katz, the FBI placed an electronic recording device outside several telephone booths where Mr. Katz made incriminating phone calls.[158] The question at issue in this case was whether the placement of the recording device on the outside of the telephone booth violated Mr. Katz' Fourth Amendment right against an unreasonable search and seizure.[159] While the parties engaged in debate regarding whether a public place should be afforded constitutional privacy protections, it was Justice Harlan's concurring opinion that created the lasting "reasonable expectation of privacy" test that has remained so prevalent among privacy discussions over time.[160] Pursuant to the test, whether an individual right to privacy exists in a situation requires two questions be asked: (1) does that person have an actual, subjective expectation of privacy, and (2) is that expectation of privacy one that society is prepared to recognize as "reasonable"?[161]

---

[152] Gostin, *supra* note 135 at 321.
[153] 5 U.S.C. § 552a.
[154] *Id*.
[155] U.S. Dep't. of Health, Education and Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems: *Records, Computers and the Rights of Citizens*, (1973) [hereinafter "H.E.W. Report"] https://www.justice.gov/opcl/docs/rec-com-rights.pdf (last visited July 2, 2019).
[156] *Id*.
[157] *Katz v. United States*, 389 U.S. 347, 348 (1967).
[158] *Id*. at 349.
[159] *Id*. at 354.
[160] *Id*. at 360; *Harlan concurring.*
[161] *Id*.

B. Heightened Expectation of Privacy of Medical Records

Following the decision in *Katz*, the U.S. Department of Health, Education and Welfare released their report of the Secretary's Advisory Committee; "There is widespread belief that personal privacy is essential to our well-being — physically, psychologically, socially, and morally… Safeguards must therefore focus on the protection of personal privacy."[162] In my view, Charles Fried captured the foundation of the 'right to privacy' when he stated, "Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."[163] Following this logic, it is still left to be determined what *type* of information should be protected and kept secret. According to the *Katz* decision, information of which one has a "reasonable expectation of privacy" should be safeguarded.[164] Given the court decisions in the cases discussed in Section III however, it seems that courts are not prepared to recognize that a fundamental right to privacy will always exist when it comes to monitoring, tracking, or disclosing medical information when it is for the purpose of furthering a state interest.

In *U.S. v. Westinghouse Elec. Corp*, on the other hand, the United States Court of Appeals for the Third Circuit explicitly recognized the existence of privacy of medical records in the context of the employer-employee relationship.[165] The court applied a seven factor analysis to determine whether employee medical records should be afforded special protections.[166] In short, defendant-employer Westinghouse Electric Corporation challenged a district court's order allowing the National Institute for Occupational Safety and Health ("NIOSH") to obtain multiple employee's medical records in an effort to investigate a complaint that employees at the Westinghouse manufacturing plant were having a reaction to a potentially toxic substance.[167] Employer Westinghouse refused to honor the subpoena and order unless, (1) the employees provided written consent to the release of the information, and (2) NIOSH provided written assurances to Westinghouse that the records would not be disclosed to third parties.[168] Most importantly, the court noted in its analysis, "there can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection."[169] It also aptly pointed out that, "it has been recognized in various contexts that medical records stand on a different plane than other relevant material."[170] The court relied on a seven factor analysis to consider whether an intrusion into an individual's privacy is justified.[171] "The factors which should be considered…are the type of records request[ed], the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other

[162] H.E.W. Report, *supra* note 155.
[163] Charles Fried, *Privacy*, 77 YALE L.J. 3, 483 (1968).
[164] *Katz*, 389 U.S. at 360.
[165] *Westinghouse*, 638 F.2d at 577.
[166] *Id.* at 578.
[167] *Id.* at 572.
[168] *Id.* at 573.
[169] *Id.* at 577.
[170] *Id.*
[171] *Id.* at 578.

recognizable public interest militating toward access."[172] The court ultimately required Westinghouse to produce the employee medical record information to NIOSH because the examination of the records was to be conducted for the purpose of evaluating potential harm to individual employees.[173]

Of importance in this 1980 case is the similarity of the seven factor test to the Health, Education and Welfare's 1973 Fair Information Practices. If you'll notice, each require adequate data storage protections to prevent unauthorized use or disclosure of the information. *Westinghouse* illustrates that, generally speaking, there is a recognized heightened expectation of privacy for medical information.[174] As such, given the type of information contained within PDMPs, sometimes highly sensitive in nature, individuals would reasonably expect that this information should remain private and confidential. When individuals seek medical treatment, they assume that they are well within the trusted realm of doctor-patient confidentiality, and that information divulged during their doctor's visit be kept private in nature, and free of judgment.[175] During a patient's visit with a physician, the patient does not voluntarily or expressly consent to their prescription information being transmitted to and stored within a state-wide PDMP tracking database. In some cases, patients are completely unaware that this information is being shared with others, and they are unable to see who requests access to their prescription drug records.[176] One would think that the type of information stored in this database would be the sort of information that is afforded a "reasonable expectation of privacy" as established by *Katz*. The seven factor analysis in *Westinghouse* and the Health, Education and Welfare's Fair Information Practice Principles highlight very important privacy standards that individuals have come to expect. They both focus on the importance of individuals being able to find out what information is being stored about them and how it is being used.[177] Most importantly, the Fair Information Practices teach us that organizations that store individualized data must take precautions to prevent unauthorized use of data.[178] Unfortunately, however, these functions are not being accomplished by PDMPs because there are no state or federal regulatory controls in place that require such safeguards or restrictions.

VI. Third-Party Access and Use of PDMP Data

A. Law Enforcement Access

As previously noted, states have a "legitimate interest" in monitoring the prescription drug use of individuals.[179] This "legitimate interest" essentially means that each state's government has an interest in promoting public health, safety, and welfare.[180] This has been accomplished by each state enacting its own PDMP, which "centralizes *all* dispensing data generated within a state (and

[172] *Id.*
[173] *Id.* at 581.
[174] *Id.* at 577.
[175] Beletsky, *supra* note 138 at 143.
[176] Nick Budnick, *Oregon's Prescription Tracking Program Monitors Your Meds*, OregonLive: The Oregonian, July 6, 2011, https://www.oregonlive.com/health/index.ssf/2011/07/oregons_prescription_tracking.html (last visited July 2, 2019).
[177] H.E.W. Report, *supra* note 155.
[178] *Id.*
[179] *Whalen*, 429 U.S. at 605.
[180] Gostin, *supra* note 135 at 87-88.

sometimes across states)… most are fully electronic and searchable, for instance by prescriber, pharmacy, or patient name."[181] While this may be the established law, *Westinghouse* dictates that certain factors should be analyzed before an intrusion into one's privacy may be appropriate.[182] A couple of these factors involve assessing the potential for harm if re-disclosed, and the adequacy of safeguards in place to prevent unauthorized disclosure to third parties.[183] Further, the Fair Information Practices dictate that individuals should be afforded the opportunity to prevent information being stored about them from being used for another non-consensual purpose.[184] Thus, some of the greatest privacy arguments against PDMPs have come into play when data within a PDMP has been accessed and used for law enforcement purposes, and not for public health purposes, as they were originally intended.[185] "If law enforcement and licensing officials are given access to the files absent any probable cause or reasonable restrictions around terms of access, PDMPs could easily turn into a tool primarily used to troll for criminal or medical misconduct."[186] This has only recently become an issue because now the majority of state PDMPs allow law enforcement officials to obtain access to its system without first obtaining a warrant.[187] As of August 2018, thirty four states permit law enforcement agencies to perform unlimited PDMP searches on any individual as long as there is an "active investigation" open.[188] Certain states, however, have chosen to specifically exclude access for law enforcement purposes.[189] On the other hand, California's PDMP, CURES, is actually housed within a law enforcement agency itself.[190] The state of Washington's PDMP is solely funded by law enforcement agencies.[191] Some state PDMPs track and monitor drug convictions or other drug charge information as well as the usual state wide prescribing information.[192] This "blurring of the lines" between health care and law enforcement has presented a number of problems, in addition to privacy concerns.[193] First, patients have become deterred from obtaining health care treatment, such as substance abuse treatment, because they fear a level of stigmatization.[194] Law enforcement access to PDMPs cause a possible "chilling effect" on prescribing and filling practices alike because patients and doctors know they are being "watched."[195] In turn, this causes physicians to limit their prescribing practices in ways that may affect their ability to provide adequate medical care.[196]

---

[181] Haffajee, *supra* note 1 at 1659.
[182] *Westinghouse*, 638 F.2d at 578.
[183] *Id*.
[184] H.E.W. Report, *supra* note 155.
[185] Beletsky, *supra* note 138 at 167.
[186] Haffajee, *supra* note 1 at 1657.
[187] Beletsky, *supra* note 138 at 167.
[188] 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* 6 (2014), http://www.namsdl.org/library/884CB2C5-1372-636C-DD54DCC00FD31313/ (last visited July 5, 2019).
[189] Butler, *supra* note 31 at 446.
[190] *See e.g.* Cal. Health & Safety Code § 11165.1; Rivais, *supra* note 73 at 60-61.
[191] Carol M. Ostrom, *New Prescription Monitoring Draws Complaints*, The Seattle Times, January 3, 2012, https://www.seattletimes.com/seattle-news/new-prescription-monitoring-draws-complaints/ (last visited July 5, 2019).
[192] Beletsky, *supra* note 138 at 169.
[193] *Id*. at 167.
[194] *Id*. at 167-168.
[195] Rivais, *supra* note 73 at 63.
[196] Haffajee, *supra* note 1 at 1657.

This "chilling effect" was addressed in the 2017 case of *Lewis v. Superior Court*.[197] Following a complaint to the medical board by a patient of Dr. Lewis, the California Medical Board initiated an investigation and obtained a copy of Dr. Lewis's prescribing history, which contained information regarding hundreds of patients.[198] Dr. Lewis argued that the board violated his patients' privacy rights because the investigator obtained the PDMP report without a warrant, subpoena, or good cause.[199] The court recognized that "it is true that the disclosure of information from the CURES database may chill patients' willingness to pursue treatment."[200] However, the court disagreed with Dr. Lewis, and concluded that the invasion of privacy in this case was justified by the state's interest in "protecting the public against incompetent, impaired, or negligent physicians."[201] *Lewis* provides evidence that individual PDMP records will not be afforded privacy protections, even in tangential circumstances such as this case which illustrates a scenario where an investigation is conducted of a physician, however, hundreds of patient prescription records were exposed in the process.[202]

B. Oregon v. United States DEA Cases

Recall from Section II, that the primary purpose of PDMPs is to mitigate prescription drug misuse by assisting physicians in understanding what drugs are being dispensed to their patients.[203] The CDC has even described the PDMP effort as "the most promising state level intervention to improve opioid prescribing…and protect patients at risk."[204] Given however that the majority of PDMPs allow law enforcement access to its system "as a matter of course," some argue that PDMPs are becoming "a tool of the police rather than an important component of patient safety."[205] This issue was addressed most recently in the state of Oregon. By way of background, the Oregon legislature created its PDMP in 2009, and it became fully operational in 2011.[206] Similar to other states, Oregon's PDMP is operated by the Oregon Health Authority, which maintains records regarding prescription drugs classified in Schedules II through IV under the Controlled Substances Act.[207] Seven million prescription records are reported to the Oregon PDMP annually.[208] Among the personally identifying information that must be reported to the Oregon state PDMP are: name, address, phone number, date of birth, and sex of the patient for whom the prescription drug was prescribed.[209] Additionally, pharmacies in Oregon must also report, within seventy two hours to the PDMP: pharmacy name, date of dispense, quantity of drug dispensed, number of refills permitted, the national drug code, and the prescribing physician's name.[210] Of great importance to the Oregon cases I will discuss is that under Oregon's PDMP law, all prescription monitoring

---

[197] *Lewis v. Superior Court*, 3 Cal. 5th 561, 220 Cal. Rptr. 3d 319, 397 P.3d 1011 (2017).
[198] *Id.* at 1015.
[199] *Id.*
[200] *Id.* at 1019.
[201] *Id.* at 1016.
[202] *Id.* at 1023.
[203] Haffajee, *supra* note 1 at 1637.
[204] CDC State PDMPs, *supra* note 58.
[205] M. Mofizul Islam & Ian McRae, *An Inevitable Wave of Prescription Drug Monitoring Programs in the Context of Prescription Opioids: Pros, Cons and Tensions*, BMC 15 PHARMACOL. TOXICOL. 46, 3 (2014).
[206] Or. Rev. Stat. § 431.962.
[207] *Id.* § 431A.855.
[208] Vivian, *supra* note 69 at 44-46.
[209] Or. Rev. Stat. § 431A.860(1)(a).
[210] *Id.* § 431A.860(1)(b).

information reported to its PDMP is considered "protected health information" under Oregon's state privacy law.[211] Federal and state privacy laws will be more thoroughly addressed in Section VII, however for the purpose of this discussion, Oregon state law defines "protected health information" as "individually identifiable health information that is maintained or transmitted in any form of electronic or other medium…"[212] Under Oregon law, "protected health information" must be safeguarded from unlawful use or disclosure and may not be disclosed except in very limited circumstances.[213] Most notably, information in the PDMP may not be disclosed unless there is a valid court order, based on probable cause, and issued at the request of a federal, state or local law enforcement agency that is engaged in a drug related investigation.[214]

On two separate occasions in September of 2012, the DEA issued administrative subpoenas to the Oregon PDMP, "demanding a summary of all prescription drugs prescribed by two physicians."[215] The Oregon PDMP refused to produce the information because it argued that to do so would violate Oregon's law which states that protected health information contained in the PDMP may not be disclosed without a valid court order, based on probable cause.[216] The difference between an administrative subpoena and a court order is such that the standard for issuance of an administrative subpoena is much lower than that of a court order.[217] Administrative subpoenas must only satisfy a "reasonable relevance" test in order for the Attorney General to issue a subpoena.[218] The United States Attorney General may "subpoena witnesses, compel the attendance and testimony of witnesses, and require the production of any records…for which the Attorney General finds relevant or material to an investigation."[219] The standard for obtaining a court ordered warrant, however, is much higher. To obtain a warrant, it must be shown that there is reasonable or probable cause to issue an order that allows for the search or seizure of information.[220] Further, an independent, unbiased judge must also determine "that there is a reasonable basis to believe a crime is being committed."[221]

In the 2014 case of *Oregon Prescription Drug Monitoring Program v. United States DEA*, the state of Oregon filed suit in federal court asking for it to determine whether the DEA's "administrative subpoena power" preempted Oregon state law, which would then require the Oregon PDMP to produce the prescribing information to the DEA, per their request.[222] The American Civil Liberties Union ("ACLU") intervened and asserted its privacy interest in the Oregon PDMP, alleging that there would be Fourth Amendment privacy rights violations against four different individuals it was representing in the matter.[223] The ACLU believed that the PDMP database risked violating the rights of Oregonians, which far outweighed any benefits it may

---

[211] *Id.* § 431.966(1).
[212] *Id.* § 192.556.
[213] *Id.* § 192.553.
[214] *Id.* § 431.966(2)(a)(D).
[215] *Or. Prescription Drug Monitoring Program ("PDMP") v. United States DEA*, 998 F. Supp. 2d 957, 961 (2014).
[216] *Id.*
[217] Vivian, *supra* note 69 at 44-46.
[218] *United States DOJ v. Utah DOC*, U.S. Dist. LEXIS 118470, 17-18 (2017).
[219] 21 U.S.C.S. § 876(a).
[220] U.S. Const. amend. IV.
[221] Vivian, *supra* note 69 at 44-46.
[222] *Or. PDMP*, 998 F. Supp. 2d at 960.
[223] *Id.* at 961.

provide.[224] The court evaluated whether the Oregon individuals contained in the database had a "reasonable expectation of privacy" of their prescription drug records under the *Katz* rationale.[225] It found that the "intervenors subjective expectation of privacy in their prescription information [was] objectively reasonable."[226] The court noted, "it is more than reasonable for patients to believe that law enforcement agencies will not have unfettered access to their records."[227] It also recognized that "prescription information maintained by [the] PDMP is intensely private as it connects a person's identifying information with the prescription drugs they use."[228] Thus, the court concluded that the DEA's use of the administrative subpoena to obtain PDMP records in this case violated the Fourth Amendment right to privacy protections, and the Oregon PDMP was justified in its refusal to disclose the PDMP information.[229] Unfortunately, however, this court decision was short lived. This decision was reversed in 2017 when the United States Court of Appeals for the Ninth Circuit held that the DEA's federal administrative subpoena power preempted Oregon's state law requiring a warrant to gain access to the PDMP.[230] In its decision, the court also found that the ACLU, as intervenors, lacked standing in requesting relief under the Fourth Amendment.[231] Thus, the current precedent in the state of Oregon is such that the DEA does not require a warrant or court order in order to gain access to and search Oregon's PDMP.[232] Despite the fact that the primary purpose of the Oregon PDMP is to provide physicians and pharmacists an avenue to improve health care, information contained in a PDMP is now likely to be subject to warrantless searches, without probable cause, by law enforcement agencies.[233]

C. Third-Party Doctrine

The *Oregon* cases have set an important standard going forward. The purpose of the probable cause requirement of the Fourth Amendment is to prevent "arbitrary or groundless government searches, for the purpose of gathering evidence for a criminal prosecution."[234] Allowing the government to invade one's right to privacy of their medical information "opens the door" to these groundless searches.[235] Of note in each case, the DEA argued that individuals should not have a "reasonable expectation of privacy in information held by a third party."[236] This "third-party doctrine," which originated in criminal procedure rules, presumes that information held by third parties shall not be afforded Fourth Amendment protections.[237] Such third parties in

---

[224] Christian Gaston, *Oregon Sues DEA Over Access to Patient Drug Records*, OregonLive: The Oregonian, November 30, 2012, https://www.oregonlive.com/politics/index.ssf/2012/11/oregon_sues_dea_over_access_to.html (last visited June 26, 2019).
[225] *Or. PDMP*, 998 F. Supp. 2d at 963.
[226] *Id.* at 961.
[227] *Id.*
[228] *Id.*
[229] *Id.*
[230] *Or. Prescription Drug Monitoring Program ("PDMP") v. United States DEA*, 860 F.3d 1228, 1237 (2017).
[231] *Id.* at 1234.
[232] *Id.* at 1235.
[233] *Or. PDMP*, 998 F. Supp. 2d at 961.
[234] Unger, *supra* note 3 at 376.
[235] *Id.*
[236] *Or. PDMP*, 998 F. Supp. 2d at 967.
[237] Wendy K. Mariner, *Reconsidering Constitutional Protection for Health Information Privacy*, 18 U. PA. J. CONST. L. 975, 996 (2016).

these instances may include hospitals and health insurers.[238] In the *Oregon* cases, the DEA contended that the third-party doctrine overrides any expectation of privacy that may have existed.[239] However, the idea that any third party falls outside the scope of patient privacy protections is just not reasonable.[240] The Fair Information Practices speak directly to the concept of the third-party doctrine. "There must be a way for an individual to prevent collected information from being used for another non-consensual purpose," and "there must be a way for individuals to know what information is being stored about them and how it is being used."[241] Thus, privacy is not merely the lack of sharing or disclosure of personal information, however, it is the control that individuals have over the information that is stored about them.[242] Allowing law enforcement "unfettered access" to PDMP records is "functionally the same as allowing the government to seize the information directly from the person."[243] Unfortunately, individuals do not have a choice as to whether their prescription drug use information gets reported to the PDMP, as pharmacies and physicians alike are required to report this information under state law.[244] "The overarching goal of PDMPs is not to operate as a law enforcement tool but to serve as a clinical instrument to help identify abuse and misuse of controlled substances."[245] Medical information disclosure for law enforcement purposes contradicts the entire purpose why each state has implemented a PDMP in the first place, to improve population health, in light of the overuse of prescription medications.[246]

VII. Federal and State Privacy Laws

A. The Health Insurance Portability and Accountability Act

The federal Health Insurance Portability and Accountability Act, ("HIPAA") was originally enacted in 1996, and was thereafter amended over time, but most notably amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act in 2009.[247] Then, in January of 2013, the Department of Health and Human Services released the HIPAA "final rule," also called the Omnibus Rule, which implemented key aspects of the HITECH Act."[248] HIPAA regulates how "covered entities" and "business associates" use and disclose "protected health information" ("PHI").[249] Protected health information is defined as "individually identifiable health information that is: (i) transmitted by electronic media, (ii) maintained in electronic media, or (iii) transmitted or maintained in any other form or media."[250] PHI includes health information data that "relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or

---

[238] *Id.*
[239] *Or. PDMP*, 998 F. Supp. 2d at 966.
[240] Jamie Wells, *Big Brother's Latest Blow To Patient Privacy*, American Council on Science and Health, August 23, 2017, https://www.acsh.org/news/2017/08/23/big-brothers-latest-blow-patient-privacy-11724 (last visited June 26, 2019).
[241] H.E.W. Report, *supra* note 155.
[242] Fried, *supra* note 163 at 483.
[243] Mariner, *supra* note 237 at 1008.
[244] *See e.g.* Fla. Stat. § 893.055.
[245] Masse, *supra* note 28 at 237.
[246] Haffajee, *supra* note 1 at 1635.
[247] 42 USC § 139 w-4(0)(2).
[248] *Id.*
[249] 45 C.F.R. § 160.103; § 164.104.
[250] *Id.* § 160.103.

future payment for the provision of health care to an individual."[251] Under HIPAA, health plans, health care providers, and health care clearinghouses (e.g. a billing service that processes PHI) are considered "covered entities," that must ensure there are proper administrative, technical and physical safeguards within an organization that guard against potential risks of unauthorized disclosure of PHI.[252] Health care providers under HIPAA include: doctors, clinics, dentists, chiropractors and pharmacies, so long as they transmit information in an electronic form.[253] "Business Associates" are entities that perform services for covered entities, that require routine access to a covered entity's protected health information in order to perform their contracted services.[254] Business associates also include any subcontractors that "create, receive, maintain, or transmit protected health information on behalf of the business associate."[255] The scope of HIPAA today is now comprised of the Privacy Rule, the Security Rule and the Enforcement Rule, which includes the new version of the Breach Notification Rule.[256] The Privacy Rule sets the standards for who may have access to PHI and sets forth the requisite safeguards.[257] The Security Rule focuses on administrative, technical and physical safeguards, specifically as they relate to electronic PHI ("ePHI").[258] The Breach Notification Rule sets standards for when individuals must be notified of an unauthorized use or disclosure of their PHI by a covered entity or a business associate.[259] HIPAA regulations are enforced by the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS").[260] OCR has the power to conduct a compliance review or an audit of an entity to ensure it is in compliance with HIPAA.[261] OCR may also conduct investigations of entities pursuant to complaints it receives.[262] Following either an investigation or a compliance review, OCR may enter into a settlement agreement, also known as a resolution agreement, in which the covered entity or business associate agrees to comply with certain obligations and corrective actions, generally for a period of three years.[263] OCR may also impose civil money penalties for violations of the HIPAA rules, depending on the severity of the violation.[264] During the 2018 year, OCR either reviewed or investigated a total of over thirty two thousand cases.[265] OCR reached large settlement amounts in ten of these cases, and obtained one

[251] *Id.*
[252] *Id.* § 160.103; § 164.500 *et seq.*
[253] *Id.* § 160.103.
[254] *Id.*
[255] *Id.*
[256] 45 C.F.R. Part 164.
[257] *Id.* § 164.500 *et seq.*
[258] *Id.* § 164.302 *et seq.*
[259] *Id.* § 160.404.
[260] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; [hereinafter "HIPAA Final Rule"]; 17 Fed. Reg. 78, 5639 (January 25, 2013).
[261] 45 C.F.R. § 160.308.
[262] *Id.* § 160.306.
[263] U.S. Dep't of Health & Human Services, *Resolution Agreements & Civil Money Penalties*, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html (last visited July 5, 2019).
[264] 45 C.F.R. § 160.404.
[265] U.S. Dep't of Health & Human Services, *Enforcement Results by Year*, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html (last visited July 5, 2019).

judgment, which totaled over twenty eight million dollars in 2018, which surpassed the previous record from year 2016 by twenty two percent.[266]

B. The Privacy Rule

Any business associate that stores, processes or has access to a covered entity's PHI must comply with many of the same requirements under HIPAA.[267] Further, covered entities must ensure that their business associates have adequate protections in place, and those business associates must ensure that all of their agents or subcontractors with which they share PHI are bound by the same requirements.[268] In order to fulfill this obligation under HIPAA, a covered entity must execute a contract with each of its business associates called a "business associate agreement," which states, among other requirements, that the business associate agrees to comply with certain provisions according to HIPAA.[269] Covered entities and business associates may not use or disclose PHI in such a way that is not specifically permitted under the HIPAA Privacy Rule.[270] Specific allowances include uses and disclosures for purposes of: treatment, payment and health care operations (such as care coordination and other general administrative activities).[271] Covered entities may also disclose PHI in other limited circumstances, such as when it is directly to the individual, and as required to comply with other applicable laws.[272] Generally speaking, any other use or disclosure not specifically permitted by the Privacy Rule requires an individual's written authorization.[273] After written authorization is obtained, any use or disclosure of PHI must be consistent with that same authorization signed by the individual.[274] Outside the scope of these permitted allowances, any "acquisition, use or disclosure of PHI in a manner not permitted by the [Privacy Rule] which compromises the security or privacy of PHI" is considered a breach, which will require notification to the affected individual and to OCR.[275] Prior to the Omnibus Rule, HIPAA dictated that a breach occurred when a disclosure of PHI "posed a significant risk of financial, reputational, or other harm to the individual."[276] Now, instead, there is a *presumption* that a breach has occurred when any PHI disclosure is made contrary to the Privacy Rule.[277] In essence, the Omnibus Rule strengthened privacy standards by implementing a more objective breach standard.[278] According to HHS, the "major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information

---

[266] U.S. Dep't of Health & Human Services, *OCR Concludes 2018 with All-Time Record Year for HIPAA Enforcement*, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/2018enforcement/index.html (last visited July 5, 2019).
[267] 45 C.F.R. § 164.314.
[268] *Id.*
[269] *Id.*
[270] *Id.* § 164.502.
[271] *Id.*
[272] *Id.*
[273] *Id.* § 164.508.
[274] *Id.*
[275] *Id.* § 164.402.
[276] HIPAA Final Rule, *supra* note 260 at 5639.
[277] *Id.* at 5641.
[278] *Id.* at 5566.

needed to provide and promote high quality health care and to protect the public's health and well-being."[279]

The HIPAA Privacy Rule also requires that covered entities and business associates, when using or disclosing PHI, make "reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose."[280] For example, if a subcontracted entity does not require an identified list of individuals in order to perform their contracted service, then that entity must not provide the identified list to that subcontracted entity. This rule, called the "minimum necessary rule," is a key protection of the HIPAA Privacy Rule, based on confidentiality concepts that essentially dictate that PHI should not be used or disclosed when it is not necessary in order to satisfy a particular purpose or to carry out a service.[281] Covered entities and business associates must develop and implement policies and procedures in order to limit uses and disclosures of PHI to the minimum necessary standard.[282] There are, of course, limitations and exceptions to the rule, such as disclosures to or requests by a health care provider for treatment purposes.[283] Generally speaking, however, covered entities and business associates must be mindful of the PHI they are using, disclosing, and requesting, and must ensure that they are not violating the minimum necessary rule in their day to day practices both internally and externally.

The HIPAA Privacy Rule also grants specific rights to individuals, including the right to access their PHI, the right to amend their PHI record, and the right to obtain an accounting of disclosures of their PHI.[284] First, individuals have a right to access, inspect, and obtain a copy of their PHI that is held in a "designated record set."[285] A designated record set is a group of records maintained by a covered entity or a business associate that is used to make decisions about individuals, such as: medical and billing records, or enrollment and claims information.[286] Once requested, an entity must act and respond to such request no later than thirty days after receipt of the request.[287] There are very limited exceptions to this rule, whereby an individual's request to access their records may be denied, such as if the record includes psychotherapy notes.[288] Individuals also have the right to have their PHI in a designated record set amended or corrected, if that information is inaccurate or incomplete.[289] Covered entities must permit individuals to make this request, and must honor the request no later than sixty days after receipt of such request.[290] Again, there are very limited circumstances in which an amendment would not be permitted, such as if the amendment to the PHI is not part of the applicable designated record set.[291] Lastly, under HIPAA, individuals have the right to obtain an accounting of disclosures of their PHI, which includes all disclosures the entity made for the last six years prior to the date of

[279] Office of Civil Rights, U.S. Dep't of Health & Human Services, *OCR Privacy Brief, Summary of the HIPAA Privacy Rule*, 1 (2003) [hereinafter "OCR HIPAA Privacy Rule"] https://www.hhs.gov/sites/default/files/privacysummary.pdf (last visited July 5, 2019).
[280] 45 C.F.R. § 164.502(b).
[281] U.S. Dep't of Health & Human Services, *Minimum Necessary Requirement*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html (last visited July 5, 2019).
[282] 45 C.F.R. § 164.316.
[283] *Id.* § 164.502(b)(2)(i).
[284] *Id.* § 164.524; § 164.526; § 164.528.
[285] *Id.* § 164.524(a)(1).
[286] *Id.* § 164.501.
[287] *Id.* § 164.524(b)(2).
[288] *Id.* § 164.524(a)(1)(i).
[289] *Id.* § 164.526.
[290] *Id.* § 164.526(b)(2).
[291] *Id.* § 164.526(a)(2)(ii).

the request.[292] While there are certain exceptions to this rule as well, generally speaking, covered entities and business associates must provide individuals with specific information in the accounting of disclosures such as the date of disclosure, the name of the entity or person who received the PHI, a description of what PHI was disclosed and what the basis for the disclosure was.[293] Of note, however, an entity does not have to include in an accounting of disclosures, any disclosures that were made for the purposes of treatment, payment, or health care operations.[294]

The Privacy Rule also requires health plans and providers to distribute a written notice to individuals that describes all of the aforementioned rights that individuals have with regard to their PHI.[295] This is called a "notice of privacy practices," which also explains how PHI is used and disclosed by the organization.[296] The notice of privacy practices is required to contain specific information contained in the HIPAA statute, including a statement that reads: "this notice describes how medical information about you may be used and disclosed and how you can get access to this information, please review it carefully."[297] Both covered entities and business associates must develop and implement internal written privacy policies and procedures that describe these items, among others, according to the Privacy Rule.[298] All employees and other members of an entity's workforce must undergo training on the policies and procedures, and there must be disciplinary action taken against any employee who violates the policies or procedures.[299] Additionally, entities must designate a privacy official that is responsible for ensuring compliance with the company's policies, who is also responsible for addressing any complaints made by individuals, and providing individuals with information they request, and also with information regarding the entity's privacy practices.[300]

C. The Security Rule

When HIPAA was implemented in the mid-1990s, Congress likely did not contemplate that the future of health care would include things such as electronic health records, or "EHRs." Thus, HHS later issued security regulations in order to establish a national standard for the protection of PHI that is stored and transmitted in electronic form.[301] According to HHS, "a major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care."[302] Generally speaking, the Security Rule includes various measures that covered entities and business associates must take in order to protect the integrity, confidentiality and availability of electronic PHI that it creates, receives, maintains or transmits.[303] Depending on certain factors, such as the size and complexity of the organization, an entity must ensure it implements any security measures

---

[292] *Id.* § 164.528(a)(1).
[293] *Id.* § 164.528(b)(2).
[294] *Id.* § 164.528(a)(1)(i).
[295] *Id.* § 164.520.
[296] *Id.*
[297] *Id.* § 164.520(b)(1)(i).
[298] *Id.* § 164.530(i).
[299] *Id.* § 164.530(b) & (e).
[300] *Id.* § 164.530(a).
[301] *Id.* § 164.302 *et seq.*
[302] U.S. Dep't of Health & Human Services, *Summary of the HIPAA Security Rule*, [hereinafter "HHS HIPAA Security Rule"] https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited July 5, 2019).
[303] 45 C.F.R. § 164.306.

that are reasonable and appropriate for the organization in order to protect against anticipated threats to the security of PHI.[304]

The Security Rule focuses on administrative, technical and physical safeguards, specifically as they relate to e-PHI, and does not apply to PHI transmitted verbally, in writing or in paper form.[305] From an administrative perspective, similar to the Privacy Rule, the Security Rule also requires covered entities and business associates to implement policies and procedures in accordance with the Security Rule, and to train all employees and members of the workforce.[306] Additionally, entities must designate a security official, who will be responsible for developing and implementing the policies.[307] Covered entities and business associates must also apply disciplinary action against employees who fail to comply with such policies.[308] Policies and procedures under the Security Rule must be intended to "prevent, detect, contain, and correct security violations."[309] This requires entities to conduct thorough risk assessments on a routine basis, in order to discover any potential risks or vulnerabilities to the confidentiality or integrity of e-PHI.[310] Under the Security Rule, "confidentiality" means that e-PHI shall not be available or disclosed to unauthorized individuals.[311] "Integrity" of e-PHI means that the e-PHI is not altered or destroyed in an unauthorized manner.[312] During a thorough risk assessment, covered entities and business associates must evaluate the probability and estimated impact of potential risks to e-PHI, and implement appropriate security measures to address the risks that were identified in the risk assessment.[313] This is an ongoing process and should be periodically re-visited and reviewed by covered entities and business associates to ensure adequate security measures remain in place.[314]

From a physical and technical safeguard perspective, and in order to comply with the minimum necessary rule, covered entities and business associates must regularly review records on all information systems to ensure there are appropriate access controls in place on each employee's computer or laptop.[315] This will ensure that electronic access to PHI is only given to employees and other workforce members based on their specific job requirements, (also called "role-based access") and that only authorized individuals are able to view e-PHI on a need-to-know basis.[316] There must also be a process by which organizations may view and examine all user access activity on their systems in such a way that it may audit logs showing who has accessed what e-PHI from a historical perspective.[317] Covered entities and their business associates must also have policies in place that govern the receipt, removal, transfer and disposal of any hardware and other electronic media that contains e-PHI within the organization.[318] Lastly, an entity must also ensure there are technical security measures in place to guard against unauthorized access to

---

[304] *Id.* § 164.306(b).
[305] *Id.* § 164.302 *et seq.*
[306] *Id.* § 164.316.
[307] *Id.* § 164.308(a)(2).
[308] *Id.* § 164.308(a)(1)(ii)(C).
[309] *Id.* § 164.308(a)(1)(i).
[310] *Id.* § 164.308(a)(1)(ii).
[311] *Id.* § 164.304.
[312] *Id.*
[313] *Id.* § 164.306(b)(iv).
[314] *Id.* § 164.306(e).
[315] *Id.* § 164.308(a)(4).
[316] *Id.* § 164.308(a)(4)(i).
[317] *Id.* § 164.312(b).
[318] *Id.* § 164.310(d).

e-PHI while it is transmitted electronically.[319] Typically, this is done in the form of encryption, whereby an organization adopts a system that has the capability to encrypt an electronic message and its corresponding attachments in such a way that only the intended authorized individual may view it.[320]

D. Business Associate Direct Liability

Another important aspect of the Omnibus Rule was that it made business associates of covered entities directly liable for compliance with certain parts of the Privacy and Security Rules.[321] The Omnibus Rule also expanded the definition of "business associate" to include any subcontractors that create, receive, maintain or transmit PHI on behalf of a business associate.[322] Expanding liability to business associates and subcontracted business associates not only increased privacy and security protections beyond covered entities, but it also allows OCR to directly regulate those entities.[323] This means that OCR may conduct investigations or audit business associates as well as their associated covered entities. Very recently, in May of 2019, HHS released further guidance regarding what aspects of HIPAA are to be imposed directly upon business associates.[324] In its press release, HHS clarified that OCR has the authority to take "enforcement action" against business associates for certain HIPAA Privacy and Security Rule requirements .[325] These requirements include: the failure to comply with the Security Rule, the failure to provide notification to a covered entity in the event of an unauthorized use or disclosure, and the failure to comply with the minimum necessary rule.[326] OCR may also impose direct liability on business associates for any failure to provide an accounting of disclosures to individuals or for failure to provide a copy of electronic PHI to either the covered entity or the individual.[327] Most importantly, in the event of an impermissible use or disclosure of PHI not in accordance with its business associate agreement or the Privacy Rule, OCR may choose to take enforcement action, including the imposition of civil money penalties directly against the business associate at fault.[328] Lastly, business associates are charged with the responsibility to ensure there are business associate agreements in place with all of its subcontractors with whom it shares PHI.[329] A failure to enter into a business associate agreement with these subcontracted entities may subject the business associate to liability and penalties imposed by OCR.[330]

The intent behind the imposition of direct liability of certain portions of HIPAA upon business associates and their subcontractors was "to avoid having privacy and security protections for PHI lapse, merely because a function is performed by an entity that is a subcontractor rather

---

[319] *Id.* § 164.312(e).
[320] *Id.*
[321] HIPAA Final Rule, *supra* note 260 at 5566.
[322] *Id.* at 5573.
[323] *Id.*
[324] U.S. Dep't of Health & Human Services, *New HHS Fact Sheet on Direct Liability of Business Associates Under HIPAA*, May 24, 2019, https://www.hhs.gov/about/news/2019/05/24/new-hhs-fact-sheet-on-direct-liability-of-business-associates-under-hipaa.html (last visited July 5, 2019).
[325] *Id.*
[326] *Id.*
[327] *Id.*
[328] *Id.*
[329] *Id.*
[330] *Id.*

than an entity with a direct relationship with a covered entity."[331] More specifically, "allowing such a lapse in privacy and security protections could allow business associates to avoid liability…"[332] The liability standard has a broad reach in that liability for any impermissible uses or disclosures "attaches immediately when a person creates, receives, maintains or transmits PHI on behalf of a covered entity or business associate and otherwise meets the definition of a business associate."[333] Direct application of HIPAA to business associates removes any type of "third-party doctrine" issue, meaning that just because information is being held by a third-party entity without a direct relationship with the individual, does not absolve that entity from any liability it may incur for improper disclosure of PHI, at least under HIPAA.

E. State Privacy Laws and HIPAA Preemption

In most circumstances, state laws that conflict with HIPAA regulations are preempted by the federal requirements, which means that state laws will not apply, and HIPAA will instead apply.[334] This is because HIPAA was created to establish "a floor of Federal privacy protections and individual rights with respect to individually identifiable health information held by covered entities and their business associates."[335] However, in the event a state law, which relates to the privacy of individually identifiable health information, is more stringent than that of the Privacy Rule, then the state law will control and HIPAA will not apply for purposes of that conflicting provision.[336] For example, it is said that the Illinois Personal Information Protection Act ("PIPA") is one of the most stringent data breach laws in the United States.[337] This is likely because the Illinois PIPA has a much broader definition of "Personal Information," and it also has a higher standard of notice obligations to individuals affected by a breach of their Personal Information.[338] Under the Act, "Personal Information" includes: first initial and last name in combination with any one or more of several data elements, including, but not limited to: social security number, driver's license number, credit card number, medical information or health insurance information.[339] This is a much more expansive definition than that of Protected Health Information under HIPAA.[340] In the event of a breach of Personal Information under Illinois state law, the data collector must provide notification to the Illinois resident "in the most expedient time possible and without unreasonable delay.."[341] On the other hand, HIPAA requires that following the discovery of a breach of PHI, covered entities are required to notify individuals "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."[342] Thus, if a breach of PHI or Personal Information occurred that affected an Illinois resident, that entity would be required to

---

[331] HIPAA Final Rule, *supra* note 260 at 5572-5573.
[332] *Id.* at 5573.
[333] *Id.* at 5598.
[334] 45 C.F.R. § 160.203.
[335] U.S. Dep't of Health & Human Services, *How does the HIPAA Privacy Rule Reduce the Potential for Conflict with State Laws?* [hereinafter "HIPAA Privacy Rule and State Law"] https://www.hhs.gov/hipaa/for-professionals/faq/401/how-does-hipaa-reduce-the-potential-for-conflict-with-state-laws/index.html (last visited July 5, 2019).
[336] 45 C.F.R. § 160.203(b).
[337] IL 815 I.L.C.S. § 530.
[338] *Id.* § 530/5.
[339] *Id.*
[340] 45 C.F.R. § 160.103.
[341] IL 815 I.L.C.S. § 530/10.
[342] 45 C.F.R. § 164.404(b).

follow Illinois state law with respect to breach notification, because Illinois state law is more stringent than that of HIPAA.[343]

Another example where a state provides far more stringent data protection laws than that of HIPAA is the California Consumer Privacy Act ("CCPA").[344] While the CCPA does not become effective until January 1, 2020, it will give California consumers a great deal of control over their information when it comes into effect.[345] As an example, the CCPA provides consumers with the right to request that a business delete any personal information about them that the business had previously collected.[346] It also has a much more expansive definition of what "Personal Information" entails, much like the Illinois PIPA.[347] The CCPA will also give California consumers the right to request that a business disclose to individuals the type of personal information that it collects, and the specific purpose for which it was collected.[348] The CCPA, however, exempts certain entities from its statutory reach.[349] More specifically, the CCPA will "not apply to protected health information that is collected by a covered entity…governed by the privacy, security, and breach notification rules…"[350] Thus, covered entities that are already subject to HIPAA will not be required to comply with the California Privacy Law.

Although there is some clarity around when a federal versus a state's privacy law will apply, it remains unclear how covered entities such as providers and pharmacies are able to provide prescription information to its corresponding state PDMP without violating applicable federal or state privacy regulations. However, under HIPAA, outside of disclosures made for treatment, payment, and healthcare operations, there are other specific exclusions whereby a covered entity may disclose PHI without receiving individual permission.[351] Of note, a covered entity, such as a doctor's office or a pharmacy, may disclose PHI without prior authorization when required by law, or for "health oversight activities."[352] Health oversight activities include disclosures to agencies that are necessary under the law to oversee the health care system.[353] Either of these exceptions under the HIPAA Privacy Rule are broad enough such that they could apply to a PDMP's operations. Additionally, a contrary state law will not be preempted by HIPAA if the Department of Health and Human Services determines that the provision of law is necessary "(i) to prevent fraud and abuse related to the provision of or payment for health care; or…(iv) for purposes of serving a compelling need related to public health..."[354] Since PDMPs were created in an effort to further population health, this exception may also apply, which will allow providers and pharmacies to provide the data to the PDMP.[355] Lastly, a contrary state law will also not be preempted by HIPAA in cases where the conflicting provision "has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances…or that is deemed a controlled substance by state law."[356] This exception

---

[343] *Id.* § 160.203(b).
[344] California Consumer Privacy Act of 2018, A.B. 375 (effective January 1, 2020).
[345] Cal. AB 375 (2018).
[346] *Id.* § 1798.105.
[347] *Id.* § 1798.135(o).
[348] *Id.* § 1798.110.
[349] *Id.* § 1798.145(c).
[350] *Id.*
[351] 45 C.F.R. § 164.512.
[352] *Id.*
[353] *Id.* § 164.512(d).
[354] *Id.* § 160.203(a)(1).
[355] Haffajee, *supra* note 1 at 1635.
[356] 45 C.F.R. § 160.203(a)(2).

seems to speak directly to state PDMPs. As such, based on these limited exceptions, covered entities such as providers and pharmacies are required to comply with state PDMP reporting laws that appear to be in conflict with the federal HIPAA Privacy Rule.

Next, it is important to understand how data contained in a PDMP is managed, stored, and maintained. As previously discussed, there are certain state PDMP laws that attempt to address the confidential nature of the information it contains, such as the California's CURES database, which references that its operation shall comply with applicable federal and state privacy and security laws.[357] Also, if you recall Oregon's PDMP law, which specifically classifies PDMP information as "protected health information" under Oregon state law.[358] This, of course, did not prevent the disclosure of PDMP information to law enforcement.[359] In a much different example, Florida law actually requires its PDMP system to "comply with the Health Insurance Portability and Accountability Act (HIPAA) as it pertains to protected health information (PHI), electronic protected health information ("ePHI"), and all other relevant state and federal privacy and security laws and regulations."[360] This appears to be a more serious effort to keep PDMP information from being disclosed to unauthorized individuals. Alabama's PDMP, on the other hand, law simply states that the information contained in its PDMP shall be "privileged and confidential," and "is not subject to subpoena or discover in civil proceedings and may only be used for investigatory or evidentiary purposes related to violations of state or federal law…"[361] It is important to note, especially with regard to Alabama's PDMP law that mere "confidentiality" of records affords a much lower standard of protection than that of PHI under HIPAA. PHI under HIPAA may not be disclosed without prior written authorization except in certain limited circumstances, such as for treatment, payment and health care operations.[362] HIPAA also requires physical, administrative and technical safeguards to be put into place in order to remain in compliance with both the Privacy and Security rules.[363] As such, simply delineating PDMP records as "confidential" does not seem like a sufficient protection for the type of individually identifiable health information contained in PDMPs.

While these PDMP statutes, on their face, appear to strive for some level of protection of the data they maintain, the PDMP entities remain unregulated, as they are not subject to oversight by any state or federal privacy authorities, such as OCR in the federal HIPAA context. This is primarily because PDMPs are neither considered a "covered entity" nor a "business associate" under HIPAA, and thus they fall outside the scope of federal privacy protections. HIPAA is a federal law that provides a uniform floor of privacy protection for individually identifiable health information in the United States.[364] Unfortunately, however, PDMPs do not fall within the scope of entities that are required to conform to these federal privacy standards.

[357] Cal. Health & Safety Code § 11165(c)(1).
[358] Or. Rev. Stat. § 431.966(1).
[359] *Or. PDMP*, 860 F.3d at 1235.
[360] Fla. Stat. § 893.055(2)(a).
[361] Ala. Code § 20-2-215.
[362] 45 C.F.R. § 164.502.
[363] *Id.* § 164.308; § 164.310; § 164.312.
[364] *Id.* § 160.103.

VIII. PDMPs Lack Privacy and Security Standards

PDMPs were created by individual states in response to the Controlled Substances Act, and the worsening opioid epidemic.[365] PDMPs may offer one of the most promising state level programs to help improve opioid prescribing and population health, however, this public health surveillance effort does not come without serious privacy or security concerns.[366] The state of Missouri was the last state to implement its own PDMP in 2017.[367] This is not because Missouri was not suffering from opioid related issues, however, Missouri Senators were instead concerned about privacy issues.[368] Ultimately, Missouri passed its PDMP regulation, noting that "the risk of encroachment on Missouri citizens' personal liberties is outweighed by the public health benefit achieved by implementing a PDMP."[369] Missouri was concerned, however, with incidents such as the Florida database leak, where over three thousand Florida residents' personal information, including list of prescription medications dispensed, was revealed to the public as part of a criminal investigation.[370] In 2013, The Florida Department of Health's prescription database leak caused a Daytona defense attorney, Michael Lambert, to file a lawsuit.[371] Mr. Lambert's lawsuit alleged that Florida's PDMP invaded individual privacy rights and subjected people to "unreasonable searches."[372] Mr. Lambert's prescription drug records were among those of the over three thousand other records who were searched as a result of an investigation by law enforcement that ultimately led to the prosecution of six people.[373] Following the Florida PDMP leak, "the American Civil Liberties Union of Florida demanded a federal investigation, and critics pointed to the incident as evidence that the system was fundamentally flawed…"[374] A similar issue also occurred in Utah, when law enforcement officials "tapped into records of almost 500 fire department employees" without a warrant or probable cause.[375] Law enforcement accessed the state PDMP database in order to investigate any firefighters who may have been obtaining prescription drugs under false pretenses.[376] It is these type of cases that illustrate that most individuals have what we've come to recognize as a *reasonable expectation of privacy* of their prescription drug records, and thus they do not expect that those records will be exposed to third parties, or the public.[377]

HIPAA was enacted to establish a "floor" of privacy protections, however, the HIPAA Privacy and Security Rules do not apply to PDMPs.[378] This essentially means that PDMPs are not required to have administrative, technical or physical safeguards in place which protect

---

[365] Unger, *supra* note 3 at 347.
[366] CDC State PDMPs, *supra* note 58.
[367] Masse, *supra* note 28 at 226.
[368] *Id*.
[369] *Id*.
[370] *Id*. at 227.
[371] Frank Fernandez, *Daytona Attorneys Pill Database Lawsuit Dismissed*, The Daytona Beach News-Journal, February 19, 2014, https://www.news-journalonline.com/article/LK/20140219/News/605060022/DN/ (last visited July 5, 2019).
[372] *Id*.
[373] *Id*.
[374] John Cox, *Did Florida's Prescription Pill Database Really Spring a Leak?* Tampa Bay Times, July 8, 2013, http://www.tampabay.com/news/politics/did-floridas-prescription-pill-database-really-spring-a-leak/2130108 (last visited July 5, 2019).
[375] Masse, *supra* note 28 at 227.
[376] *Id*.
[377] *Katz*, 389 U.S. at 389.
[378] HIPAA Privacy Rule and State Law, *supra* note 335.

individually identifiable prescription drug information. By way of illustration, a covered entity (such as a pharmacy or a doctor's office), is required by state law to report prescription information including, but not necessarily limited to: name, address, phone number, date of birth, prescription drug name, prescriber name, quantity, and number of refills to the state run PDMP.[379] As previously noted, the covered entity in this scenario is acting in accordance with HIPAA, because HIPAA allows disclosures as required by law or for purposes of serving a "compelling need related to public health."[380] Then, the protected health information is transferred and stored in an electronic database within each state.[381] PDMPs contain individually identifiable health information, sometimes sensitive in nature, as they collect and store information regarding what prescription drugs are prescribed and dispensed to patients.[382] At this stage, the PDMP is an entity that one would reasonably infer should be considered a "business associate" under HIPAA, since it maintains and processes PHI it receives from covered entities; however, PDMPs do not fall within the Privacy Rule (or the Security Rule) because they are neither considered a "business associate" nor a "covered entity" under HIPAA.[383] Further, PDMPs are thus not regulated by the Department of Health and Human Services, OCR, or by any other regulatory authority.[384] While prescribers (physician's offices) and dispensers (pharmacies) are clearly subject to HIPAA regulations, the entity collecting information from these sources (state PDMP) is not subject to HIPAA.[385] This is an obvious privacy "lapse," which ultimately creates a risk of exposure of some of the most sensitive PHI.[386] This concept is in sharp contrast with the purpose of HIPAA and its corresponding Omnibus Rule, which in recent years has expanded its reach to not only regulate covered entities but also directly regulate business associates and their subcontractors.[387] Instead, PDMPs are allowing a "lapse" in privacy and security protections; the very same type of "lapse" that the Omnibus Rule intended to eliminate.[388]

More importantly, the HIPAA Privacy Rule provides individuals with certain rights, such as the right to access your own information, the right to amend your information, and the right to obtain an accounting of disclosures to understand who has been provided with access to your information.[389] Charles Fried captured this concept of 'right to privacy' when he explained that the fundamental meaning of privacy centers around the ability we have to control what information is being stored about ourselves.[390] PDMPs, however, do not provide individuals with any of these rights or controls. Covered entities and business associates, throughout their day-to-day use and disclosure of PHI are also required to keep that use or disclosure to the minimum amount of information necessary in order to pursue a specific intended purpose.[391] There are no privacy standards, however, that are afforded to individuals when PDMPs either choose to or are required to disclose information to third parties, including law enforcement.[392] Additionally, in order to

---

[379] Or. Rev. Stat. § 431A.860.
[380] 45 C.F.R. § 160.203(a)(1).
[381] *See e.g*. Fla. Stat. § 893.055.
[382] Unger, *supra* note 3 at 347.
[383] 45 C.F.R. § 160.103.
[384] Wood, *supra* note 7.
[385] *Id*.
[386] Cox, *supra* note 374.
[387] HIPAA Final Rule, *supra* note 260 at 5566.
[388] *Id.* at 5573.
[389] 45 C.F.R. § 164.524; § 164.526; § 164.528.
[390] Fried, *supra* note 163 at 483.
[391] 45 C.F.R. § 164.502(b).
[392] *Or. PDMP*, 860 F.3d at 1235.

remain in compliance with the Privacy Rule standards, covered entities and business associates are required to designate a privacy official, who enforces the requisite policies and procedures, including imposition of disciplinary sanctions for violation of such policies and procedures.[393] PDMPs are not required to follow these same rules, and there are no individuals dedicated to enforcing privacy or security standards at PDMPs.

PDMPs have made efforts that attempt to reach a level of privacy, such as exempting prescription data from public records laws, or including provisions that punish wrongful receipt of PDMP information.[394] Unfortunately, however, without any state or federal oversight, or a universal privacy standard imposed upon PDMPs, there are no incentives for states to comply with appropriate privacy standards. Further, PDMPs are not required to notify individuals or any regulatory agency in the event of a breach of individually identifiable prescription drug information or other PHI. Information reported in PDMPs can reveal a great deal of information regarding a patient's medical status, including the specific condition for which they are being treated.[395] This includes, but is not necessarily limited to: psychiatric disorders, chronic pain disorders, substance use disorders, gender identity disorder and AIDS.[396] Even though medical records are typically afforded a "heightened expectation of privacy,"[397] PDMPs are not required to abide by the same restrictions that are placed upon business associates and covered entities, and they face no penalties in the event of unauthorized disclosure.

Thus far I have focused on the privacy concerns with regard to how PDMPs operate, however, there are legitimate security concerns that center around the vulnerability of PDMPs as electronic databases.[398] Dating back to 1974, Congress found, when it enacted the Federal Privacy Act, that the expansion of technology, including the use of computers has "greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information."[399] In 2009, as part of the American Recovery and Reinvestment Act, Congress enacted the Health Information Technology for Economic and Clinical Health ("HITECH") Act.[400] The HITECH Act was created to expand the adoption of health information technology solutions throughout the health care system and incentivize health care organizations to implement Electronic Health Record ("EHR") systems.[401] Covered entities and business associates utilize EHR systems to keep up to date information on a patient's entire medical record including: medical history, diagnoses, medications, and laboratory and test results.[402] The implementation of EHRs was intended to improve health care quality and reduce errors and advance the overall delivery of health care.[403] Similarly, state PDMPs are currently operated on electronic platform systems, and contain first and last names of individuals, their address, phone number, date of birth, and prescription drug history including prescriber and quantity dispensed.[404] Each state's PDMP stores statewide prescription drug dispensing information in an aggregated

[393] 45 C.F.R. § 164.530(a).
[394] Unger, *supra* note 3 at 363.
[395] *See e.g. Doe,* 72 F.3d at 1135.
[396] Margo, *supra* note 52 at 1593.
[397] *Westinghouse,* 638 F.2d at 577.
[398] Unger, *supra* note 3 at 352.
[399] 5 U.S.C. § 552a.
[400] 42 USC § 139 w-4(0)(2).
[401] *Id.* § 139 w-4(0)(2), Subtitle A.
[402] Office of Nat'l Coordinator for Health Information Technology, *What is an Electronic Health Record?* https://www.healthit.gov/faq/what-electronic-health-record-ehr (last visited July 7, 2019).
[403] 42 USC § 139 w-4(0)(2), Subtitle A.
[404] *See e.g.* Or. Rev. Stat. § 431A.860.

form, which can be accessed by various users.[405] Unfortunately, however, state PDMP systems are not required to follow the comprehensive administrative, physical or technical safeguard standards of the HIPAA Security Rule, nor are they subject to the HITECH Act.[406] As such, Information stored within the PDMP is at risk for cyberattacks, unauthorized hacking, or other misuse of the information.[407] A case example of this occurred in June of 2009, when the state of Virginia experienced an incident where a computer hacker was able to gain access to the prescription drug records of millions of individuals.[408] According to reports, the hacker claimed he had access to more than thirty five million prescription records and demanded a ten million dollar ransom.[409] Once stolen, such records could potentially expose Virginia residents to medical identity theft, if an unauthorized individual contacted a pharmacy to request a refill, for example.[410]

PDMPs present the possibility for security breaches, where private prescription drug information may be disclosed to the general public.[411] In fact, Congress introduced a bill a few years ago that would have created a requirement that all state PDMPs must share their data across state lines, with other states.[412] The Prescription Drug Monitoring Act of 2017 would have required the establishment of "an inter-state data sharing single hub to facilitate the sharing of PDMP data among states and the accessing of such data by practitioners."[413] Even though this bill did not pass the House of Representatives, some states currently voluntarily share PDMP data with other states via a system called "PMP InterConnect," which facilitates the transfer of PDMP data across state lines and allows participating states from across the nation to be linked.[414] All states should realize that inter-state sharing of PDMP data is likely to be a potential requirement in the future. Nationwide PDMP data exchange only amplifies the need for data security protections to avoid inappropriate disclosure of PDMP information.[415]

As they currently stand, PDMPs collect and store statewide prescription drug data, which is aggregated in a database that may be widely accessed by many different types of authorized users.[416] That being said, PDMPs, unlike covered entities and business associates under the Security Rule, are not required to conduct risk assessments in order to ensure that the confidentiality and integrity of the information that it holds remains intact.[417] PDMPs are also not required to implement access controls, nor are they required to audit historical access activity, to ensure that no unauthorized individuals have accessed or viewed prescription drug records.[418] HHS has said that the goal of the Privacy Rule is to protect patient information and promote public health while promoting quality health care.[419] Similarly, the goal of the Security Rule is to allow

---

[405] Rivais, *supra* note 73 at 60-61.
[406] 45 C.F.R. § 164.308; § 164.310; § 164.312.
[407] Wood, *supra* note 7.
[408] Dutko, *supra* note 33 at 756.
[409] Bill Sizemore, *Hacking of Prescription Database May Lead to Headaches*, The Virginian-Pilot: Health and Medicine, May 8, 2009, https://pilotonline.com/news/local/health/article_eaf700ca-ea49-5e20-bf00-aae75a11ea04.html (last visited July 7, 2019).
[410] *Id.*
[411] Haffajee, *supra* note 1 at 1656.
[412] Prescription Drug Monitoring Act of 2017, 115 S. 778 (2017).
[413] *Id.*
[414] HHS OIG Oversight of Opioid Prescribing, *supra* note 30.
[415] Haffajee, *supra* note 1 at 1662.
[416] *Id.* at 1656.
[417] 45 CFR § 164.308(a)(1)(ii).
[418] *Id.* § 164.308(a)(4); § 164.312(b)
[419] OCR HIPAA Privacy Rule, *supra* note 279.

entities to adopt technologies to improve the quality and efficiency of care.[420] Ironically, the purpose of PDMPs is nearly the same; PDMPs were created to protect patients at risk for overdosing, and also to improve individual and population level health.[421] However, PDMPs are failing to protect the PHI that it is required to collect and store. PDMPs are escaping privacy and security standards and safeguards. This failure to safeguard patient data has the potential to do much more than harm individual privacy rights, but it also can potentially undermine patient trust and can push patients away from seeking the medical attention they need.[422]

IX. Recommendation

From a public health perspective, PDMPs were created as a response to the opioid epidemic, which has proven to be a worsening crisis over time.[423] That being said, PDMPs collect and maintain what is considered "protected health information" under HIPAA; however, PDMPs fall outside the scope of control by regulatory agencies. As such, privacy and security protection of the data stored within PDMPs remains unaddressed at this time. In terms of their structure, PDMPs reside within state Departments of Health, or within law enforcement agencies.[424] Since PDMPs do not reside within healthcare institutions, they are not covered by HIPAA or any other federal or state provisions that protect personal health information.[425] This failure to adequately address and protect individual rights and confidentiality can eventually generate negative impacts on a population level.[426] Despite that fact that some states have structured their PDMP laws in an attempt to move toward confidentiality of records, I believe that federal action is long overdue. Measures should be taken to protect both the privacy and the security of individual PDMP records.[427] In doing so, all states should, at the very least, be required to align their privacy and security standards with federal standards, such as the HIPAA Privacy and Security Rule.[428] Requiring state PDMPs to provide assurances that their systems are in compliance with HIPAA, would solve privacy concerns for both patients and providers.[429] Not only would individuals have more control over their information that is stored within PDMPs, but the PDMP itself would be required to undergo periodic risk assessments to ensure that any vulnerabilities are addressed and that the electronic databases remain secure from potential unauthorized access or breach of information.

If PDMPs were brought under HIPAA legislation, it would require a significant revision to the HIPAA statute, specifically to the definition of what is considered a "covered entity."[430] As it currently stands, HIPAA "covered entities" do not encompass or contemplate the concept or structure of PDMPs.[431] However, a national comprehensive framework is necessary in order to

[420] HHS HIPAA Security Rule, *supra* note 302.
[421] Haffajee, *supra* note 1 at 1635.
[422] Beletsky, *supra* note 138 at 142.
[423] 21 U.S.C.S. § 801.
[424] Beletsky, *supra* note 138 at 165-166.
[425] *Id.*
[426] *Id.* at 147.
[427] Butler, *supra* note 31 at 446.
[428] *Id.*
[429] Wood, *supra* note 7.
[430] 45 C.F.R. § 160.103.
[431] *Id.*

afford privacy and security protections to the data that is stored within PDMPs.[432] Thus, HIPAA should be amended to include PDMPs within the definition of a "covered entity." Additionally, the meaning of "healthcare operations" would likely require expansion if PDMPs were brought within the HIPAA definition of "covered entity" because PDMPs will require the ability to conduct their day to day operations without violating the Privacy Rule. Clearly, certain regulatory details and language would need to be clarified, however, establishment of this federal floor of protection would provide a solid baseline for privacy and security protections of prescription drug information captured by state PDMP databases. It would also reduce the variability between state PDMP laws, and provide one national standardized system of afforded protections.[433] In the world of health care, it has been recognized for some time that personally identifying medical information shall be afforded heightened protections. When it comes to the personal identifying information contained in PDMPs, however, there is an obvious lack of direction and regulation; PDMPs are escaping privacy protections. Classification of PDMPs as a "covered entity" under HIPAA would effectively empower federal regulators to exercise oversight and control of these entities to ensure they are in compliance with privacy and security rules and protections.

[432] Kathryn M. Marchesini, *IMS Health, Inc. v. Ayotte: Small Step for Privacy, Giant Leap Still Needed for Prescription Data Privacy*, 10 N.C. J.L. & TECH. ON. 96, 111-112 (2009).
[433] Rivais, *supra* note 73 at 63.