TESTIMONY OF ANDREA MEYER
IN OPPOSITION TO

SB 355: STATE PHARMACY DATABASE LAW

BEFORE THE SENATE COMMITTEE ON HUMAN SERVICES AND RURAL HEALTH POLICY

FEBRUARY 9, 2009

The ACLU of Oregon strongly opposes SB 355 and urges this Committee not to pass this bill out in any form.

INTRODUCTION

SB 355 would create a government-monitored database in Oregon on our lawful prescriptions. It interferes with patient/doctor relationship, puts medical and personal identifying information at risk, provides broad access to providers and pharmacies while denying consumers any notice, meaningful remedy if wrongly identified or recourse for negligent or reckless release of data.

The current proposal would authorize the "State Board of Pharmacy to establish, maintain and operate an electronic system *to monitor and report drugs of concern with a documented potential for abuse* that are dispensed by prescription." The determination of what drugs have a potential for abuse will be made exclusively by the board.

SB 355 is far more expansive than previous proposals, which have been limited to Schedule II, III and IV controlled substances. In 2007, the proponents testified that such a database would include 2-5 million "if not more" prescriptions a year. In all likelihood with the much broader scope of drugs that can be included in this database, it is fair to expect significantly more than 2-5 million prescriptions to be databased a year under this plan. Some of the most frequently prescribed drugs were already included under the previous proposal, including all codeine-based products, Xanax, Ambien, Vicodin and Ritalin (which will result in databasing children).

This law would give blanket authority to the board to determine which drugs constituted "potential for abuse" and could not only cover a very wide range of

non-controlled substances but potentially become a politicized decision depending on the beliefs of the decision makers at the board at any given time. With a population under 4 million in Oregon and a database containing

millions of prescriptions a year, it is reasonable to ask exactly how many Oregonians will be databased under this law. Or maybe the question to ask is who *wouldn't* be in this database.

While federal and state officials argue the database is needed to deter abuse by drug-seeking patients, the result is that the database will treat almost if not *all* Oregonians as potential drug-seeking abusers. In a time when technology gives the government (as well as the private sector) the increasing ability to reduce our right to privacy, it is worth remembering the words of former U.S. Supreme Court Justice Louis Brandeis, who in 1890 wrote that the right to privacy is "the most comprehensive of rights and the right most valued by civilized man." This cherished right is now under attack, and one of the primary culprits is the government and its desire, often well-intentioned, to use the advance of technology to monitor our activities to help us, deter crime or find the ones who are breaking the rules. The result is a slow but steady erosion of our privacy, subjecting us not only to invasion but real risks.

The existence of a government database may interfere with a doctor/patient relationship. Some may be afraid to work with a doctor to seek necessary pain medication, anxiety medicine, sleep medication, or any other condition for which a drug is databased, if this information will be second-guessed and potentially shared with law enforcement by government officials.

PRESCRIPTION PROGRAMS ARE UNPROVEN

At the December 2008 conference put on by the Pain Commission and Board of Pharmacy, one of the keynote speakers stated that there has been very little research available to guide this program and there has been no outcome evaluation of the Harold Roger grants. The other keynote speaker said that if these programs are administered improperly it undermines pain management and proper prescribing. The program administrator from Virginia said that no one has used the program data to advocate for more treatment and there's no data to show that these programs have improved access to care or drug treatment.

The bottom line is these programs have been heavily advanced by the offer of a federal grant from the Department of Justice, the law-enforcement, not health care arm of our federal government. Despite the expansion of these programs, no one knows whether they truly work. Oregon shouldn't join a program that has not been found to be effective.

CONFIDENTIAL INFORMATION CAN NOT BE FULLY PROTECTED

In this day and age, the same technology that allows the government to collect and database this type of sensitive information, such as medical history and personal identifying information, makes it difficult protect from security breaches.

The types of security breaches run the gamut and include breaches that occur on-line data transmission, emails, hacking, compromised passwords, stolen equipment, lost equipment, illegitimate access by former employees and dishonest insiders.

According to the Privacy Rights Clearinghouse, in the first 36 days of 2009, there have been 36 breaches across this country (this is consistent with an average breach a day for the past few years). Of those 36, *three* occurred in Oregon: University of Oregon (Jan 13), Southwestern Oregon Community College (Jan 16) and the most recent at the Coos Bay Department of Human Services (Jan. 30) where a scammer made off with Social Security numbers after sending a virus online to a computer at the Department of Human Services office. An application that was installed recorded keystrokes and sent them to an external address.

Neither the health care industry nor governments are immune. In the past 4 months there have been 53 breaches reported by health care systems or state and federal government entities (well over 50% of the breaches that have occurred in that period of time). The list includes: Oregon Health and Sciences University (December 2008), the Veterans Affairs Medical Center in Portland (November 2008), as well as Bayside Medical, Cedar-Sinai Medical Center, Mary Washington Hospital, Medical Mutual of Ohio, Baylor Health Care System, the Kanasha-Charleston Health Dept., the New Hampshire Department of Health and Human Services, the North Carolina Department of Health and Human Services and the Madison Human Resources Department.

The proponents may argue that there has been no history of data theft or hacking from pharmacy databases in other states. These recent examples of security breaches should not be ignored. Thieves were able to gain access to millions of consumer profiles including Social Security numbers, other personal identifying information, credit histories, medical information and other sensitive material. Just because it may not have happened with a pharmacy database should give us no comfort when one reviews the breadth and depth of data breaches reported since 2005.

The response to privacy and security concerns has not been adequately addressed. Until recently the proponents argued a budget of $300,000 for two years was sufficient to create and operate the database. But in March 2007 Legislative Fiscal Office stated that “The Board’s fiscal impact is premised on the $300,000 of federal grants funding it has received rather than a clearly articulated plan (and associated budget) detailing how the data will be acquired, validated, managed, stored, secured, and analyzed. Thus the actual cost of this measure, both for the 2007-09 biennium as well as beyond, is uncertain.”

Washington state’s budget analysis estimated a $2.1 million cost for the first two years of the pharmacy database program. Washington also has a $300,000 federal grant but recognized the inadequacy of that funding. “The Harold Rogers grant … would not be adequate to fund this program and, therefore, additional funding will be needed.” Washington appropriate $1 million last year to start the program. At the beginning of this year, facing a budget crisis, it suspended the program entirely.

In the past, the board has indicated its intention to contract out the database services to a private vendor. By doing this, a part of the very limited funds dedicated to a database will be directed to the profit margin of a private business. In addition, by contracting out the database services to a private party, the board reduces the level of security by requiring additional transmission of personal identifying and medical information between this new entity, the board, pharmacists and physicians. This increases the opportunity for security breaches by outside sources or negligent release internally. In addition, the board has no direct oversight over the private vendor's employees, relying on simple assurances rather than direct accountability.

LAW ENFORCEMENT INVOLVEMENT

Section 3(2)(i) gives the board authority for "developing and maintaining effective evaluation and referral mechanisms **to evaluate and refer appropriate individuals to** medical care, addiction treatment, or **law enforcement.**"

Recently, the board wrote that one of the four reasons for the database is to "recognize and identify Oregonians [who are engaged in] blatant doctor shopping or pharmacy hopping [that] is evident ***in the internal program audits."***

It seems clear that one of the goals of this proposal is to give the board and its authorized agents the authority to intervene through law enforcement with people it believes are misusing these medications. In 2005 it was framed as "A third objective is to develop greater understanding and coordination of efforts between healthcare and medical practitioners and law enforcement personnel." In 2009 it's no longer an objective but explicit authority provided in law.

A review of the program in other state raises alarm bells and suggests the real intent by the federal government for pushing state implementation of these programs is closely linked to law enforcement. Six states, including some of the largest, operate their program through law enforcement: California, New York, Pennsylvania, Texas, Hawaii, and Oklahoma.

Information through September 2006 from the National Alliance for Model State Drug Laws (which is the most recent information available) also reveals the relationship between these databases and law enforcement. In Idaho, 70% of the requests are from law enforcement. In Illinois it is 50%. In Indiana and Pennsylvania **all** of the requests are for law enforcement purposes. Massachusetts is 61%, Mississippi is 50%, and Oklahoma is 60%. Far from focusing on drug intervention, in a number of states, the focus of this program is for law enforcement purposes.

NO CONSUMER RIGHTS AND REMEDIES

Oregonians have no meaningful rights or remedy under this proposal, as set forth below.

NO NOTICE TO CONSUMERS

Not only does SB 355 not require consent from persons prior to the entering of their information into this database, the law does not even provide *notification* of the existence and inclusion into the database. The reality is that although we are talking about this database, the vast majority of Oregonians will never know it exists.

Instead, persons should be clearly informed by the prescribing physician *prior* to the prescription, thus giving them a choice of whether or not they want that drug or another one that won't require them to be databased. If notice is not given or delayed until the person is at the pharmacy, he or she will never be able to discuss this important issue with the prescribing doctor.

OVERLY BROAD ACCESS TO DATABASE

Rather than limiting the authority to run a report on a person who is receiving a drug that is on the database, Section 5 (2)(a)(A) allows a practitioner or pharmacist to receive a report if they are "evaluating the need for or providing *medical* or pharmaceutical treatment" to a person "for whom the practitioner or pharmacist *anticipates* providing, is providing or has provided care."

In other words, if the provider or pharmacist anticipates or is providing any type of medical treatment, they can run a report. As a result, SB 355 gives the authority to a pharmacist to run a report on *every single customer*. The same is true for any provider, even if it's not relevant to the care sought.

REAL RISKS OF WRONGFUL IDENTIFICATION

It's a Friday evening and a person needs critical medication. The pharmacist checks the database and it reports multiple prescriptions for this person in a short period of time and therefore the pharmacist will not fill it. What if the database is wrong? This law allows a person to be denied lawfully prescribed medication that a doctor deemed necessary. If the patient tries to pick up the medication after-hours or on the weekend, the doctor may not be available to override the database or the pharmacist. At the December 2008 conference, the Virginia program administrator stated that their office, available to handle questions that arise from the report, is open only 9-5 Monday through Friday providing no assistance to an emergency room doctor or pharmacist faced with questionable data.

Under SB 355 the only time the pharmacy must fill a prescription, if it were otherwise going to, is if the database is actually down. Nothing prevents the pharmacy from deciding for whatever reason based on the report it receives that it will not fill a person's prescription at all or until it reaches the physician, which may not happen for hours or days. The result is people will be denied appropriate and legally prescribed medications in a timely manner.

How to ensure that John Doe is the same John Doe each time the database is queried or information is submitted, especially with millions of prescriptions a year, has not yet been answered. Multnomah County has hired experts to guide them in developing an electronic-based court filing system. The expert reported that lacking universal unique identifiers (such as SSN), person-matching errors will always exist. The question then comes, how many mismatch errors is acceptable in a pharmacy database?

What if the database releases information to a doctor or some other entity with whom the person has no relationship? What if the database releases one person's information but the request was for someone else? How will a person know if the database has provided personal medical information in error? The only way to have meaningful oversight is for the individual to receive notification each and every time a report is requested. Only the individual knows if he or she went to doctor A or picked up a prescription at pharmacy X.

NO RIGHT TO REPORT OR CORRECTIONS

While the providers and pharmacies will have access 24/7 to a person's complete information through a report with no limitation on how many times they query the database, Section 5(2)(c) provides that a person may request his or her own information in accordance with procedures established by the board only once every six months and the board can take up to 10 days after the request to provide the information. The law does not define what "information" a person has the right to see. Will that be prescription history, will it include who has requested a report in the past, and will it include any other data that is contained on their record? The law is silent so it's up to the board to decide what information the person gets.

That same subsection provides that a person may *request* the board to correct any information that the person believes is erroneous (one does not need statutory authority for that). The proposal, however, does not require the board to take action, does not set forth a time requirement to address the complaint, nor an appeal process for the person if the board refuses to take any or timely action. That is not a meaningful due process right or remedy.

RETENTION OF DATA TOO LONG

The proposal, as it stands, allows the Board to retain the data for three years, which is way too long for what will likely be tens of millions of prescriptions retained in a database at any given time.

EXTREMELY BROAD IMMUNITY PROVISION

This is one of the broadest immunity provisions possible and protects everyone but the consumer who will have no remedy for almost any kind of release and violation of this law.

The board, which will be responsible for ensuring safety and accuracy of the data, has under Section 3(2)(f) given itself authority to assess any civil penalties for failing to report or for *wrongful disclosure of data*. Does that mean the board will fine itself if it wrongfully discloses data? At a minimum the Attorney General on behalf of consumers should have authority to assess civil penalties for the board if it wrongfully discloses.

Further, "a pharmacy . . . [or] a person authorized under [Section 5] to obtain or use information from the program . . . is immune from civil liability arising out of the reporting *or* release of the information *if* the pharmacy or person reports, obtains *or* uses the data in good faith." As written, as long as the pharmacy or provider *obtains* the data in good faith or *uses* the data in good faith (either one, not necessarily both), they are immune if they negligently, recklessly or even intentionally release the data. Even if this were not to provide immunity for intentional actions, a person whose data is released by anyone because of negligence or reckless handling, has no rights or remedies despite the injury suffered.

In fact, there is no provision that consumers will ever know if there has been a wrongful release or use their information. While the board may assess a civil penalty against an actor, it has no obligation to inform anyone of the misuse. And there is no right to a separate remedy to make the consumer whole. The civil penalty will go to the state, not the individual harmed.

And SB 355 does not just include immunity to Oregon pharmacists, doctors and the State of Oregon but also provides immunity if information is negligently or intentionally released *by another state* that received the information. Under Section 5(2)(e)(E) (please note that this refers to lines 30-32 on page 3), the board is authorized to share Oregonians information with other states so long as the board determines that the security and privacy standards are "equivalent" to those of the board. Since it will be left to rulemaking to ensure any security system, there will be absolutely no check on what standards are used let alone what review will be used to determine the adequacy of another state's program.

This provision is entirely premature. The board should not be the ones designated to determine whether or not another state's database is sufficiently safe and secure. The system in Oregon is not up and running and one would hope that even the most ardent proponent of this program would agree that if Oregon develops this database it should spend the first few years ensuring sufficient protection, operation and quality control before it gets into the business of determining the adequacy of another state's program and linking its system to theirs. Nothing stops the board from seeking this authority later from the legislature when it can provide specific information about the adequacy of the other state's program.

COST

Cost related to operating this program is a critical civil liberties issue. When databases are authorized and the state is given powerful authority to collect and share personal information, it is also essential that sufficient funds be allocated to ensure that the system is the best one available and is continually updated with the state-of-the-art technology. That best technology is most often the most expensive. If Oregon moves forward, we would urge that the necessary resources be allocated. It may not be particularly difficult or expensive to put ***a*** prescription database in place in Oregon but Oregonians don't want just any system. They want one that fully protects their information from either external or internal breaches.

Other states running prescription monitoring programs have recognized this. Alabama's more limited program (Schedules II, III, IV and V, with once-a-week data collection) became fully operational in 2006. It collects 9-10 million prescriptions a year. The start-up for the program was $1,150,000. In 2008 the state appropriated an additional $525,688 for the program.

The start-up costs for Kentucky's program in 2005 was $1.4 million. Only after that original funding did the legislature allocate an additional $5 million to develop and implement additional system enhancements, including moving towards allowing the system to collect prescription data within 24 hours of dispensing. [1]

CONCLUSION

This plan is not ready to move forward and this proposal is too flawed. We do not know how this program will be run, how it will be funded or how the funding will be increased to keep up with the need to take advantage of better technology.

SB 355 is written to assist pharmacists and providers but omits any meaningful consumer protections, due process rights and remedies. Despite the good intentions of many who support it, SB 355 takes us down an extremely dangerous road. It is an unprecedented intrusion by the State of Oregon into the lawful medical information of Oregonians. For all the reasons the ACLU of Oregon urges you not to pass SB 355 in any form.

[1] The source for Alabama and Kentucky information is the National Alliance for Model State Drug Laws which assists states with the creation of prescription drug monitoring programs and the state's own prescription drug monitoring program website.