Prescription Drug Abuse and Diversion: The Role of Prescription Drug Monitoring Programs
Bill Number:
Hearing Date: September 23, 2004, 2:00 pm
Location: SD-430
Witness:
Joy L. Pritts, J.D.
Health Policy Institute, Georgetown University
Assistant Research Professor
Testimony

I. INTRODUCTION

Mr. Chairman and Members of the Committee on Health, Education, Labor and Pensions: Thank you for the opportunity to testify before you today on the need for adequate privacy protections in prescription drug monitoring programs.

My name is Joy Pritts. I am an assistant research professor at Georgetown University's Health Policy Institute. My work at Georgetown focuses on laws, policies, and practices related to the privacy of medical information.

The non-medical use of prescription drugs continues to be a widespread and serious problem in this country. As part of the effort to control the illegal diversion of prescription drugs, many states have instituted prescription drug monitoring programs. These programs collect, review, and analyze identifiable prescription data from pharmacies. Although the programs differ in terms of objectives, design, and operation, they generally analyze and distribute collected information to medical practitioners, pharmacies, and regulatory and law enforcement agencies.
Many of these programs have been successful at reducing diversion within their states. It is not surprising that expanding the number of state prescription drug monitoring programs and ensuring that they are able to share data across state lines are key elements of the federal strategy to reduce prescription drug abuse nationwide.

While the goals of these programs are admirable, increasing the number of prescription drug monitoring programs that are able to share identifiable information electronically raises serious privacy concerns. Millions of Americans suffer from chronic pain. Without adequate privacy safeguards, patients will not seek treatment and practitioners will be hesitant to adequately prescribe medication. Absent strong privacy protections, there may well be wide-spread public resistance to linking prescription drug monitoring program data.

II. THERE SHOULD BE FEDERAL PRIVACY STANDARDS FOR PRESCRIPTION DRUG MONITORING PROGRAMS

Federal proposals to encourage the expansion and linkage of state prescription drug monitoring programs should establish minimum, uniform privacy standards for these programs based on well-established fair information practice principles. Federal privacy standards for prescription drug monitoring programs are essential because these programs

generally are not subject to the Federal Privacy Rule issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA Privacy Rule). The Privacy Rule only governs three major categories of entities that maintain identifiable health information called “covered entities”: health care providers; health care clearinghouses; and health plans. Most state programs are administered by a state board of pharmacy, a state department of health, or a state law enforcement agency. As a general rule, these entities are not subject to the restrictions imposed by the HIPAA Privacy Rule.

While states generally have some privacy protections for prescription drug monitoring program data, these protections can vary widely from state to state. For example, some states impose a criminal penalty for unauthorized use or disclosure of prescription drug monitoring program information and others do not. Linking data between states with differing standards can result in decreased privacy protections for citizens of states with stringent privacy laws. Citizens should not lose privacy protections as a result of states’ sharing data. As a practical matter, states with high privacy standards may be reluctant to share data with states that have less privacy protections.

Establishing federal minimum privacy standards for prescription drug monitoring programs can help ease these concerns. While states should remain the primary regulators of prescription drug monitoring programs, any federal funds for such programs should be tied to the requirement that state programs meet minimum federal privacy standards. States should remain free to impose higher privacy standards to meet the particular needs of their citizens.

At a minimum such federal standards should:
• Provide individuals specific notice that certain prescription drug information will be reported to a state prescription drug monitoring program and may be shared with programs of other states
• Provide individuals with a right of access to their information that is maintained in a state prescription drug monitoring program and the right to contest the accuracy of the information
• Limit the information provided under these programs to the minimum amount necessary to accomplish the intended purpose
• Require recipients of information from prescription drug monitoring programs to only use the information for the purpose for which it was disclosed and prohibit them from further disclosing the information
• Establish safeguards for verifying the accuracy of reported information
• Establish security standards for maintaining and transmitting data
• Require requests for inspection from most law enforcement agencies to be reviewed and approved by appropriate officials prior to disclosure
• Require the de-identification of information provided for statistical, research, or educational purposes
• Impose stringent civil and criminal penalties on the improper use and disclosure of prescription drug monitoring program data

To the extent the federal government determines that it will directly operate prescription

drug monitoring programs, these standards should also apply to the federal program. The restrictions in the Privacy Act are insufficient.

Notice

Practitioners and/or dispensers of prescription drugs should be required to give individuals adequate notice that information related to prescriptions for certain classes of drugs will be reported to the state's prescription drug monitoring program. Individuals should be informed of who will have access to this information and the purposes for which they can use the information. Giving notice avoids any potential of "secret" databases. As a practical matter, adequate notice should also have a direct deterrent effect on "doctor shopping" because potential diverters will be made aware that their prescription drug information will be reviewed by the program and shared with other practitioners.

Most health care providers such as doctors and pharmacists already are required to give patients a notice of privacy practice under the HIPAA Privacy Rule. The HIPAA Privacy Rule, however, only requires a general notice of privacy practices that includes certain examples. To be an effective deterrent, notice of under the prescription drug monitoring program would need to specifically advise consumers that if they have certain prescriptions filled, their prescription information will be reported to the state monitoring program. Thus, notice under the prescription drug monitoring program should be in addition to the notice required by the federal Privacy Rule.

Access

Individuals should have the right to access and contest their identifiable data that is maintained in a prescription drug monitoring program. The right of access ensures that identifiable information is accurate and complete. Due to the sensitive nature of prescription drug information, it is particularly important that data collected be associated with the proper person.

Minimum Information

Only the minimum amount of information necessary to accomplish the intended purpose should be disclosed to recipients of information from prescription drug monitoring programs. This determination can be made at the policy level. The standard should apply not only to information that is requested of the program but also to any disclosures that are made as a matter of routine.

Restrictions on Recipients of Information

Federal standards should require recipients of prescription drug monitoring program information to use the information only for the purpose for which it was disclosed. They should also prohibit recipients from sharing the information with others. Kentucky's prescription drug monitoring program incorporates these protections.

Integrity

The integrity of data in a prescription drug monitoring program is vital. Programs should be required to verify the accuracy of reported information. They should be required to

either destroy old data or convert it to an anonymous form.

Security Standards

Maintaining a system of linked electronic databases with identifiable prescription drug information poses significant security risks. The information is sensitive and can potentially be improperly used against individuals. Because the information is identifiable and available in a concentrated format, it may also prove to be a tempting target both for hackers and for authorized personnel who may have improper motives to access the data. The information is a potential treasure trove for bitter ex-spouses, potential employers, and others.

Similar data has been compromised in the past. In the mid 1990's, a Florida Department of Health employee downloaded the names of over 4,000 AIDS cases from a county computer that stored mandatory reporting information on new AIDS cases and used the information for "dating" purposes. The names were also transmitted to two newspapers.

Security measures can help prevent such loss and the unauthorized access, destruction, use, or disclosure of the data. Managerial measures include internal organizational measures that limit access to data and ensure that individuals with access utilize data for only authorized purposes. Such security standards should include role-based access and procedures for verifying that those outside the organization who request information have the authority to access the information. These measures should also include periodic audits to ensure that data is being accessed appropriately. Minimum standards should also be set for the technical protection of this sensitive data, including storing data on secure servers and encrypting information in transmission.

Serious consideration should be given to the manner in which information is collected and maintained in these programs. As discussed above, central data bases with names, addresses and prescription drug information are tempting targets for security breaches. Furthermore, the very idea of centralized data bases elicits strong reaction among many individuals. In the recent debate over whether Florida would establish a central data base for prescription drug monitoring, Rep. Rene Garcia (R- Hialeah) an opponent of the program stated, "My parents fled a Communist country because everything was being centralized."

Some networks that share health information utilize other methods for linking their data. For example, the New England Health Electronic Data Interchange Network is well-known for its network which does not rely on a central database. Federal strategies to encourage the sharing of data between prescription drug monitoring programs should consider these alternative methods of exchanging data to decrease security risks.

Access by Law Enforcement

Prescription drug monitoring programs should not permit all law enforcement agencies unfettered access to collected data. Unfettered law enforcement access raises concerns from consumers and physicians that they will be improperly targeted for prosecution. Access should be limited to agencies acting within their official duties that are

conducting bona fide criminal investigations or criminal prosecutions. Law enforcement requests to inspect prescription drug monitoring program data generally should be subject to review and approval by appropriate authorities prior to disclosure. In Massachusetts, for example, law enforcement agencies must first direct their request for prescription drug monitoring program information to the Office for the Attorney General or the Massachusetts State Police Diversion Investigation Unit or the U.S. Drug Enforcement Administration for notification and approval.

Access by Researchers

Some prescription drug monitoring programs make their data available for research or education purposes. To the extent that this information is made available, it should be furnished only in de-identified form.

Enforcement

Privacy protections can only be effective if there is real enforcement. State laws vary greatly in enforcement or penalty provisions. Some appear to provide only for minimal fines such as $500.

To ensure compliance with privacy standards, punishment should be public and severe. Federal standards should provide for significant civil and criminal penalties for:

- Authorized personnel improperly obtaining, using or disclosing information from a prescription drug monitoring program
- Recipient's improperly using or disclosing information that they obtained from a prescription drug monitoring program and
- Any person's improperly obtaining or using prescription drug monitoring program information

States should, of course, remain free to provide for private rights of action.

III. CONCLUSION

Prescription drug monitoring programs appear to be an effective tool in reducing prescription drug diversion and abuse. Minimum privacy standards should be an essential component in any federal programs to encourage the expansion and interconnectivity of these programs.