HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE AND PRESCRIPTION DRUG MONITORING PROGRAMS (PMPS)

SHERRY L. GREEN, CHIEF EXECUTIVE OFFICER
NATIONAL ALLIANCE FOR MODEL STATE DRUG LAWS (NAMSDL)

Since 2004, NAMSDL has helped state and federal officials assess the applicability of state and federal confidentiality and privacy laws, regulations and rules to the interstate disclosure of dispensed substances information. A primary focus has been the potential impact of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (Privacy Rule). 45 C.F.R. Part 160 and Subparts A and E of Part 164.

REPORTING OF DISPENSED PRESCRIPTION DRUG DATA BY DISPENSER

Any review of the Privacy Rule's applicability necessarily begins with a dispenser's required reporting of specified dispensed prescription data to a PMP.

The Privacy Rule addresses the use and disclosure of protected health information (PHI) by those subject to the Privacy rule, called covered entities. Such entities include providers of medical or health services, such as physicians and pharmacists, who electronically transmit PHI in connection with transactions covered by HIPAA. These transactions are financial or administrative activities related to health care, such as coordination of benefits, health care claims or health care payments.

As noted by the Office of Civil Rights, U.S. Department of Health and Human Services (HHS), "[a] major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being." Office of Civil Rights (OCR), U.S. Department of Health & Human Services (HHS), OCR Privacy Brief, Summary of the HIPAA Privacy Rule 1 (2003).

HIPAA generally preempts a provision of state law that is contrary to a Privacy Rule standard, requirement or implementation specification. A state law requiring the transmission of specified dispensed prescription data to a PMP could potentially be deemed contrary. However, HIPAA identifies several exceptions to the preemption which may apply to PMPs. A contrary state law will not be preempted if the Secretary of HHS determines that the provision:

- is necessary (i) to prevent fraud and abuse related to the provision of or payment for health care; or …(iv) for the purposes of serving a compelling need related to public health; 45 C.F.R. §160.203(a)(1) or
- has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing or other control of any controlled substance (as defined under federal or state law). 45 C.F.R. §160.203(a)(2).

Another relevant exception which does not require a HHS determination occurs when**:**

- a provision of state law provides for reporting of disease or injury . . . or for the conduct of public health surveillance, investigation or intervention. 45 C.F.R. §160.203(c).

When no exception applies, a covered entity may only use or disclose protected health information: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing. 45 C.F.R. §164.502(a).

Under 45 C.F.R. §164.512, a covered entity may disclose PHI without receiving permission of the individual for 12 national priority purposes. These include several which may apply to a PMP's operations:

- **Disclosure required by law.** A mandate contained in law compels an entity to use or disclose information, and is enforceable in a court of law. Mandate includes a civil or authorized investigative demand, and statutes or regulations that require the production of information. 45 C.F.R §164.512(a).
- **Public Health Activities**. Disclosure may occur to an agency or authority responsible for public health matters as part of its official mandate, if the public health authority is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, . . . and the conduct of public health surveillance, public health investigations, and public health intervention. 45 C.F.R. §164.512(b), 45 C.F.R. §164.501.
- **Health Oversight Activities.** Disclosure may occur to a health oversight agency for legally authorized oversight activities. The agency must be authorized by law to oversee the health care system, whether public or private, or government programs in which health information is necessary to determine eligibility or compliance . . . . 45 C.F.R. §164.512(d), §164.501.
- **Law Enforcement.** Disclosure may occur for a law enforcement purpose to a law enforcement official under six circumstances, if applicable conditions are met. One of the designated circumstances is a disclosure as required by law. A law enforcement official is an officer empowered to

investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law. 45 C.F.R. §164.512(f), §164.501.

- **Treatment, Payment, Health Care Operations.** Disclosures are permitted for a covered entity's own treatment, payment or health operations. Health care operations include (i) quality assessment and improvement activities, including case management and care coordination, and (ii) fraud and abuse detection and compliance activities. 45 C.F.R. §164.506, §164.501.

In disclosing dispensed prescription drug data pursuant to 45 C.F.R. §164.512(b), (d), (f), or health care operations under 45 C.F.R. §164.506, a covered entity must limit the PHI to that minimally necessary to accomplish the intended purpose of the use, disclosure or request. 45 C.F.R. §164.502(b)(1).

The Health Information Technology (HITECH) Act passed as part of the American Recovery and Reinvestment Act (ARRA) adopted requirements pertaining to the minimum necessary rule. A covered entity will be deemed in compliance with §164.502(b)(1) only if PHI is limited, to the extent practicable, to the limited data set, or if needed, to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. American Recovery and Reinvestment Act (ARRA), Pub. L. No. 111-5, H.R 1 (1009), Div. A, Title XIII, Subt. D §13405(b)(1)(A). Section 13405(b)(1)(A) remains effective until new guidance on minimum necessary is issued by the Secretary of HHS. The Secretary's deadline for such issuance is August 17, 2010.

DISCLOSURE BY A PMP OF COLLECTED DATA REGARDING DISPENSED PRESCRIPTION DRUGS

After collection of specified prescription data, a PMP may re-disclose that data to the extent and in the manner prescribed by state and federal law, regulation and rule. State PMP enabling laws often incorporate particular language designed to protect confidentiality and privacy rights related to PMP information. Common statutory safeguards include:

- Designating PMP data as confidential and exempting the data from public records or open records laws.
- Carefully delineating who is allowed to access the PMP information, under what circumstances the information may be accessed or what criteria must be met for access, and for what purposes the lawfully accessed data may be used.
- Explicitly requiring that the statewide agency operating the PMP comply with all relevant state and federal privacy and confidentiality laws. Some state statutes also require that the agency develop procedures and policies which protect the confidentiality of the information.

- Penalizing the unlawful access and/or the unlawful disclosure of PMP data.

Additionally, states sometimes institute a data purging requirement. Some states purge the information in the PMP database no later than a designated number of years after the collection of the data. The range of years specified in PMP authorizing laws can vary from one to six. Even if a PMP law is silent on the issue, a purging requirement in another statute may be deemed applicable.

PMPs implement the legislative privacy protections with precise procedures for the submission of information requests and the corresponding program response. One critical procedure is the authentication, registration or authorization of individuals or entities allowed to request and use PMP data. A 2005-2006 survey of PMPs conducted by IJIS revealed that 71% of those surveyed have such procedures. The timing of authentication and the documentation which applicants for access to the PMP information must submit currently differs among states.

The categories of individuals or entities often identified as authorized requesters and users of PMP date include:

- Licensed physicians and others with authority to prescribe substances;
- Pharmacists and others with authority to dispense substances;
- Designated law enforcement officials;
- Representatives of professional or occupational licensing, certification or regulatory boards, commissions or agencies; and
- Individuals whose receipt of prescription drugs has been included in the PMP database.

States add categories of authorized users as is appropriate for that jurisdiction. For example, states using an outside vendor to collect data may allow appropriate personnel of that vendor to access the PMP information. Another example involves states that provide for an advisory committee, task force or council to work with the statewide entity housing and operating the PMP. Those states may permit advisory committee members to access the PMP data.

Jurisdictions may explicitly reference in their statutes certain out-of-state requesters that can ask for PMP data. For example, many states provide information to federal law enforcement officers, especially DEA representatives. Some states specify that a law enforcement officer from another state is eligible to receive PMP information. For example, Kentucky's law specifies that the PMP agency may provide data to a "certified or full-time peace officer of another state". KY. REV. STAT. ANN. §218A.202 (West 2009). Similarly, Indiana allows the release of PMP information to "[a] law enforcement officer who is an employee of … an entity that regulates controlled substances or enforces controlled substances rules or laws in another state". IND. CODE ANN. §35-48-7-11.1 (West 2010). Ohio's Board of Pharmacy may provide information from the

PMP database "on receipt of a request from…a state or local officer of this state or any other state…" OH CODE ANN. 4729.79 (A)(2) (West 2010). Some states specifically include licensing bodies of other states as authorized users of PMP data. For example, New Mexico's Administrative Code allows the Board of Pharmacy to provide PMP data to "professional licensing authorities of other states if their licensees practice in the state or prescriptions provided by their licensees are dispensed in the state…" N.M. CODE R. §16.19.29.9E.(4) (Weil 2010). Hawaii, Indiana, Mississippi and New Jersey are examples of states which legislatively permit controlled substance or prescription monitoring programs or authorities of other states to access PMP data. HAW. REV. STAT. § 329-104 (2009); IND. CODE ANN. §35-48-7-11.1 (West 2010); MISS. CODE ANN.§73-21-127 (West 2009); N.J. STAT. ANN. §45:1-46 (West 2009), S.B. 355, 75th Leg., §4(2)(a)(E) (Or. 2009), H.B. 1231, 85th Leg., §14 (S.D. 2010).

In jurisdictions with laws that do not specifically identify authorized out-of-state requestors, appropriate agency counsel will clarify the territorial limits of their PMPs' distribution activities. The survey by IJIS of PMP officials indicated that 59% of the PMP officials surveyed were able to fill a data request from an out-of-state PMP when the end user was a prescriber or pharmacist. Seventy-three (73%) were able to respond with information to another PMP's request when the end user was a law enforcement or regulatory agency.

Out-of-state authorized requestors and end users of data must submit to authentication processes and are often bound by the same use restrictions as their instate counterparts. Two-thirds of the states surveyed by IJIS confirmed the continuity of the restrictions regardless of the intrastate or interstate nature of the disclosure.

The HIPAA Privacy Rule may also guide the use of information released by a state PMP. As noted previously, the collection of selected prescription drug data may have occurred pursuant to a permitted disclosure provision of 45 C.F.R. §164.512. The PMP should ensure that its distribution of prescription drug information remains consistent with the purposes for which the dispenser was initially allowed to report the information without authorization of the individual.

For example, a PMP may collect data in its capacity as a lawfully authorized health oversight agency for use in its legally authorized health oversight activities. The agency may be required to protect and preserve public health and safety through regulation of the delivery of health care. To accomplish its mandate, the particular Board, Department or Bureau may license qualified health care professionals, enforce standards of practice and/or regulate the quality, manufacture, sale and distribution of prescription drugs.

The Privacy Rule encompasses these tasks within its description of health oversight activities which includes audits; civil, administrative, or criminal investigations, inspections; licensure or disciplinary actions; civil, administrative, or criminal

proceedings or actions; or other activities necessary for appropriate oversight of the health care system. 45 C.F.R. §164.512(d).

The PMP's release of collected dispensed prescription data is designed to help the PMP enhance the provision of health care and ensure the appropriation distribution of prescription drugs. Disclosure to and use by designated recipients of the information helps identify and appropriately resolve drug diversion practices, including doctor shopping, and inappropriate or inadequate prescribing or dispensing practices. As noted earlier, authorized recipients often include prescribers, dispensers, occupational licensing representatives, law enforcement officials and other PMPs.

Moreover, a PMP enabling statute may delineate the authorized requestors and end users of data, and any restrictions on the use of the prescription information. This specific language represents a conscious balance struck by the state, through a public, deliberative process, between securing the privacy of the information and allowing disclosure and use options that are necessary for appropriate oversight.

TRANSMISSION OF DATA BY A DISCLOSING PMP DIRECTLY TO AN AUTHORIZED USER WHO DIRECTLY REQUESTS THE DATA

After verifying a requestor's eligibility to receive prescription drug data, a PMP may transmit the information directly to an authorized requestor and user. The disclosing PMP should take certain steps intended to help maintain compliance by the authorized requestor and user with applicable state and federal confidentiality, privacy, disclosure and use laws. These include obtaining assurances that:

- the requestor will comply with all restrictions placed by the disclosing PMP on the use and further disclosure of information which it releases; and

- the receipt and subsequent use and disclosure of PMP data distributed by the disclosing PMP will fully comply with (1) HIPAA and (2) all pertinent laws, regulations and rules regarding the privacy, confidentiality, disclosure and use of health information enacted by the state in which the requestor is located.

TRANSMISSION OF DATA BY A DISCLOSING PMP TO AN AUTHORIZED USER VIA A REQUESTING PMP

A PMP may ask for information from another PMP on behalf of another authorized requestor and user. The disclosing PMP should obtain the assurances noted above from the PMP serving in the role of the official requestor of data. Additional agreements from the requesting PMP may be pertinent depending on the scope of its role in authenticating and communicating with the end user. The disclosing PMP may need to seek from the requesting PMP a combination of the following:

- when applicable, a certification that the end user is eligible to receive prescription data from the disclosing PMP with a detailed basis for that certification;

- when applicable, agreement to assist in gathering the necessary information and documentation for the disclosing PMP to determine the eligibility of the end user to receive prescription data;

- when applicable, agreement to communicate to the end user all restrictions placed by the disclosing PMP on the use and further disclosure of information which it releases;

- when applicable, agreement to assist the disclosing PMP in communicating to the end user all restrictions placed by the disclosing PMP on the use and further disclosure of information which it releases;

- when applicable, certification that the requesting PMP has received assurances from the end user that the receipt and subsequent use and disclosure of PMP data distributed by the disclosing PMP will fully comply with (1) HIPAA and (2) all pertinent laws, regulations and rules regarding the privacy, confidentiality, disclosure and use of health information enacted by the state in which the end user is located; and

- when applicable, agreement to assist the disclosing PMP in acquiring assurances from the end user that the receipt and subsequent use and disclosure of PMP data distributed by the disclosing PMP will fully comply with (1) HIPAA and (2) all pertinent laws, regulations and rules regarding the privacy, confidentiality, disclosure and use of health information enacted by the state in which the end user is located.

TRANSMISSION OF DATA BY A DISCLOSING PMP TO AN AUTHORIZED USER VIA A HUB SYSTEM

The IJIS Phase III project has focused on the development and operation of a pilot hub system to facilitate the exchange of PMP data among multiple requesting and disclosing PMPs. A key objective of the project is to reduce overall national request and information transmittal costs. Over 30 states now maintain operational PMPs. If a state PMP had to send a request for information regarding a particular individual separately to many PMPs, the transmittal costs could be significant.

The hub model which is the current focus of the Phase III project does not store information or engage in substantive evaluations of requests for data. It becomes part of the process for transmitting data requests and properly disclosed prescription information. Participants in the pilot hub system are limited to PMPs. Another authorized requestor

(requestor), such as a prescriber, pharmacist, or specified law enforcement official, must route a data request to his or her participating PMP for hub submission.

After the system accepts the request, the hub sends the request to all relevant disclosing PMPs. Each disclosing PMP which provides prescription data in response to a request will send the informational response to the hub. Depending upon rules of the requesting and disclosing PMPs, the hub may consolidate all or a portion of the received responses. The hub transmits all responses to the requesting PMP who communicates the information to the requestor.

The impact of the hub on privacy, confidentiality, use and disclosure compliance is related to its effectiveness in accurately and safely distributing required information among multiple participants. That effectiveness may depend on the identification and inclusion of proper structural safeguards for the scope and amount of information that is designed to flow through the hub. This is particularly so for materials regarding verification of authorized users, restrictions on the use and disclosure of data, and assurances regarding conformity with federal and state law.

The hub may send a requesting PMP the authentication requirements for each disclosing PMP to which the data request pertains. The system may be intended to relay documents from the requesting PMP to each disclosing PMP for a determination that the requestor is eligible to receive prescription data. The hub would have to distinguish among the many distinct verification requirements and send the correct materials to each disclosing PMP. Alternatively, the hub may be required to send a finding of eligibility by the requesting PMP, with the accompanying rationale, to each relevant disclosing PMP.

Some of the disclosing PMP responses which the hub receives may contain restrictions on the further use and disclosure of the data. The hub would need to obtain guarantees of compliance with the limitations prior to transmitting any restricted responses to the requesting PMP. Such a guarantee may possibly be incorporated into the format for requesting data. If consolidation of responses occurs, the hub would have to capably forward the precise limitations imposed with identification of the corresponding disclosing PMP.

The hub's ability to distinguish among state requirements plays a lesser role in assurances regarding HIPAA and the law of the state in which the requesting PMP and requestor are located. The developers of the hub could create an online certification applicable to all participating PMPs which would provide that:

- the receipt and subsequent use and disclosure by the requesting PMP and requestor, of data released by a disclosing PMP, will fully comply with (1) HIPAA and (2) all pertinent laws, regulations and rules regarding the privacy, confidentiality, disclosure and use of health information enacted by the state in which the requesting PMP and requestor are located.

Prior to signing the online certification, a participating PMP may document its receipt of compliance assurances from the requestor.

To ensure the hub's structural soundness for the contemplated information exchange, the participating PMPs may require the hub Administrator to undertake particular responsibilities. Among these are the duties:

- to provide for the functionality of the hub, including by storing and distributing business rules associated with information exchange processes;

- to duly register each participating PMP as a registered user of the hub upon execution of an appropriate agreement by such PMP, and terminate such registration upon receipt of notice from the PMP or upon the Administrator's determination that a PMP has failed to fully comply with all rules and policies required for participation in the hub; and

- to institute and maintain all necessary and proper security safeguards to allow only authorized representatives of participating PMPs to transmit and receive requests and information through the hub.

Technical standards for the sharing of health information continue to advance. PMP officials and others addressing prescription abuse, addiction and diversion must remain vigilant about privacy and confidentiality considerations. This vigilance will create opportunities to shape new technologies to best protect individuals while permitting appropriate regulation of controlled substances and prescription drugs.