



## Questions and Answers

*UPDATED: May 14, 2009*

**Q: NEW 05/14/2009- What is the current status of the Department of Health Professions data breach?**

A: The Virginia Department of Health Professions (DHP) Prescription Monitoring Program (PMP) computer system was accessed by an unauthorized user. The investigation to determine the extent of any data compromise and to identify the individual involved is being pursued aggressively by federal and state law enforcement. All PMP data was properly backed up and all back-ups have been secured. There is no evidence that systems beyond the PMP were involved.

A complete security assessment and testing of all DHP systems is being conducted. As individual systems are determined to be safe and secure by the Virginia Information Technology Agency (VITA) and law enforcement, they are being brought back online. The DHP website is now available for use by the public. The public may now safely access License Lookup, Physician's Profile, and Renew Online.

**Q: NEW 05/14/2009 - What is being done to protect patient information stored on the PMP database?**

A: The state's computer security experts and network engineers are putting in place a number of advanced measures to prevent incursions, including new firewalls, reconfiguring the network, and conducting vulnerability assessments of the agency's systems.

The system does not contain patient medical histories; it is not a medical record system nor is it tied to a medical records system. Information included in the database is limited to prescription information for covered substances only.

In the past, the use of a personal identification number, including Social Security number has been an optional data element. Only a minority of prescription records in the PMP database contain Social Security numbers. To protect against potential compromise in the future, the agency is deleting all personal identification numbers, including Social Security numbers, from the PMP database and will not accept this information as additional entries in the future.

The PMP system continues to be evaluated by VITA systems security staff and law enforcement. The PMP system will not be accessible to registered users until all security issues have been fully resolved and the system has been cleared by VITA and law enforcement.

**Q: NEW 05/14/2009 - Will the public be notified if their information is on the PMP database?**

A: The PMP database is currently being examined to identify individuals whose Social Security numbers are in the system. For the majority of persons in the database Social Security numbers were not recorded. A letter will be sent to all persons whose prescription records are determined to contain Social Security numbers to alert them of potential exposure and to advise them of precautionary steps they may take. As more information on the notification process becomes available, additional information will be provided to doctors and other prescribers and pharmacies and will be posted on the agency's website, [www.dhp.virginia.gov](http://www.dhp.virginia.gov).

**Q: What is the Virginia Department of Health Professions?**

A: The Virginia Department of Health Professions (DHP) is a state agency that licenses and regulates health care professionals in Virginia. The mission of the Department is to enhance the delivery of safe and competent health care by licensing qualified health care professionals, enforcing standards of practice, and providing information to both practitioners and consumers of health care services. One of the programs managed by the Department is the Prescription Monitoring Program.

**Q: What is a Prescription Monitoring Program (PMP)?**

A: Prescription Monitoring Programs (PMPs) are systems in which controlled prescription drug data are collected in a database, centralized by each state, and administered by an authorized state agency to promote the appropriate use of controlled substances for legitimate medical purposes, while deterring the misuse, abuse, and diversion of controlled substances. As of October 2008, 38 states had enacted legislation permitting PMPs or had operational PMPs. Each state controls the language of its PMP with regard to how the prescription information gathered as part of the program will be accessed, by whom, and for what limited purposes.

**Q: When was the Virginia PMP implemented?**

A: The Commonwealth implemented a pilot program in Southwest Virginia in September 2003, which contained information about the Schedule II controlled substances dispensed in that region. In 2006, the program expanded statewide and now includes information for prescriptions dispensed in Schedules II, III, and IV.

**Q: What kinds of drugs are in Schedules II, III, and IV?**

A: Schedule II drugs include oxycodone, methadone, morphine, Ritalin

Schedule III drugs include Hydrocodone, Vicodin, testosterone, Tylenol with Codeine

Schedule IV drugs include Valium, Xanax, Darvocet-N100, Ambien

**Q: Who has access to the data in the program?**

A: Prescribers and Pharmacists (upon providing notification of the patient and for their specific patient), certain authorized law enforcement and regulatory personnel (with an open investigation required), and patients over the age of eighteen may receive their own information. In addition, de-identified data is available for research and education purposes.

**Q: What data is collected?**

A: Pharmacies and other dispensers licensed by the Virginia Board of Pharmacy at DHP must report to the PMP twice monthly.

Required data elements include:

- Recipient's name and address
- Recipient's date of birth
- Covered substance dispensed to the recipient
- Quantity of the covered substance that was dispensed
- Date of the dispensing
- Prescriber's identifier number
- Dispenser's identifier number
- Prescription number

Optional data elements include:

- Dispenser's customer identification number, which in limited instances may be a social security number
- Number of refills authorized by the prescriber

**Q: What if I have concerns about possible identity theft?**

A: Although we are not aware of any evidence indicating any personal information may be at risk, we nonetheless recommend that you remain vigilant over the next 12 to 24 months, including carefully reviewing account statements for your financial products and services, and promptly reporting incidents of suspected identify theft to the applicable financial institution.

We also recommend that you periodically obtain and carefully review your credit report from each of the nationwide credit reporting agencies, and request that information related to fraudulent transactions, if any, be deleted from these reports. You may obtain a free copy of your credit report once every 12 months from Equifax, Experian, and TransUnion. You can request this free service by visiting the website [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling 877-322-8228, or completing the annual credit report request form available at [www.ftc.gov/credit](http://www.ftc.gov/credit).

If you find suspicious activity on your credit reports, or have reason to believe your information is being misused, contact your local police department. You should also file a complaint with the Federal Trade Commission by calling 1-877-438-4338.

As an additional precaution, you may wish to contact the three credit bureau reporting agencies to place a fraud alert on your credit file. A fraud alert makes creditors aware of possible fraudulent activity on your account, and tells creditors to contact you before they open any new accounts or change your existing accounts.

You can place a fraud alert on your credit file by contacting any one of the three major credit reporting agencies using the following contact information:

Equifax: 800-525-6285  
Experian: 888-397-3742  
TransUnion Corp: 800-680-7289

**Q: What can I do to combat medical identity theft?**

- Every year, ask your insurance company for a complete list of payments made for your medical care
- Monitor ‘Explanation of Benefits’ statements received from insurers
- Contact your insurer(s) and provider(s) about charges for care that you did not receive, even when there is no money owed
- Share personal and health insurance information only with trusted providers
- Maintain copies of healthcare records
- Check personal credit history for medical liens
- Request that providers and insurance companies correct errors and amend medical records to alert a user to inappropriate content

**Q: What are some websites that may have more information?**

Federal Trade Commission Identity Theft Website:

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

Federal Trade Commission Identity Theft Website: Identity Theft page

<http://www.ftc.gov/bcp/menus/consumer/data/idt.shtm>

AARP

[http://bulletin.aarp.org/yourmoney/scamalert/articles/scam\\_alertmedical\\_id\\_theft\\_a\\_fast\\_growing\\_crime.html](http://bulletin.aarp.org/yourmoney/scamalert/articles/scam_alertmedical_id_theft_a_fast_growing_crime.html)

**Q: What do I do if I think someone is misusing my personal information?**

A: Call the Federal Trade Commission’s ID Theft hotline at 1-877-438-4338 to make a report. TTY users should call 1-866-653-4261.

**Q: Where do I go for more information?**

A: Please visit [www.dhp.virginia.gov](http://www.dhp.virginia.gov) for more information. The website will be periodically updated with pertinent information as it is received.