Updated June 7, 2010
(bold blue indicates updated information)

Frequently Asked Questions - Updated

AvMed Information Breach

I heard that some state employees may have had personal health information stolen. How do I know if my information was exposed?

State of Florida employees and retirees who have, or had dating back to April 2003, a health insurance plan through AvMed, including Medicare, Commercial and Self-Funded options, may have some of their information exposed. These members should have received a letter in February alerting them that their information was potentially exposed. **Beginning June 7, 2010, AvMed will mail letters to another 70,461 State of Florida individuals.**

AvMed set up a toll-free hotline at (877) 263-7998 to provide affected members with what specific personal information may have been exposed.

What information was exposed? Could someone use it to steal my identity?

The information includes combinations of information including names, addresses, phone numbers, Social Security numbers and protected health information. However, because of the way this information was listed, AvMed believes the risk of identity theft is very low. **To date there is no evidence that any individuals' information on the stolen laptops has been misused since the theft occurred.**

If you are concerned that some of your information was exposed, AvMed set up a toll-free hotline at (877) 263-7998 where they can provide you with what, if any, of your personal information may have been exposed.

How many people had their information exposed by this breach?

Personal health information for 20,181 current State of Florida employee subscribers and their dependents may have been compromised initially. Another 21,215 State of Florida employees/retirees and their dependents who had AvMed coverage since 2003 may also have been impacted. **AvMed hired PricewaterhouseCoopers (PwC), an international leader in cyber security, to ensure that the AvMed conducted a thorough and accurate forensic analysis. PwC's analysis identified an additional 70,461 current or former State of Florida employees who are affected; of those, 14,437 are active AvMed subscribers and 56,024 are inactive AvMed subscribers.**

I am one of the members whose information was exposed. What are you doing to protect me?

We are committed to helping safeguard your personal information. AvMed contracted with the Debix Identity Protection Network to provide affected members with 24 months of identity protection for free. Your participation in this is not automatic. You **must** enroll in this program to receive this credit monitoring, and you have 120 days from receiving your letter to do so. You can enroll by phone at (877) 263-7998, or online at www.debix.com/safe. To register online, you need to provide the activation code

located at the top of your letter from AvMed. **Beginning June 7, 2010, AvMed will mail letters to notify these additional 70,461 affected individuals. AvMed will not send another letter to individuals who received letters in February.**

In addition, Debix notified the three credit bureaus about this incident, as well as the Centers for Medicare and Medicaid Services, and the Florida Office of Insurance Regulation.

We continue to work with the Office of Insurance Regulation to ensure that we are taking every possible step to protect State of Florida employees and retirees.

How do I get the free credit monitoring?

You **must** enroll in this program to receive this credit monitoring, and you have 120 days from receiving your letter to do so. You can enroll by phone at (877) 263-7998 or online at www.debix.com/safe. To register online, you need to provide the activation code located at the top of your letter from AvMed.

I heard this theft happened in December. Why am I just finding out about it?

While the theft happened December 11, 2009, AvMed notified the Department of Management Services Division of State Group Insurance the afternoon of Wednesday, February 3, 2010, **about the initial affected individuals**.

In December, AvMed reported the theft of the laptops to the Alachua County Sheriff's Office, and continues to cooperate with their investigation. In addition, they hired external security consultants to help conduct their investigation. **In February AvMed mailed letters to the individuals identified as being affected at that time. AvMed then hired PricewaterhouseCoopers (PwC), an international leader in cyber security, to ensure that the AvMed conducted a thorough and accurate forensic analysis. PwC's analysis identified the additional 70,461 current or former State of Florida employees who are affected.**

What if my identity has already been stolen, and my Debix monitoring just started, or hasn't started yet?

If you have any reason for concern, contact the Attorney General's Citizens Services Hotline at (866)9-No SCAM (1-866-966-7226). Additional information about protecting yourself from identity theft is available online at http://www.myfloridalegal.com/identitytheft. The Attorney General reminded all customers that if anyone calls them requesting personal information related to the breach, the call is fraudulent and you should report it to the Attorney General's Citizens Services Hotline.

How did this breach happen?

On December 11, 2009, two company laptops were stolen from an AvMed corporate building in Gainesville, Florida. AvMed notified the Department of Management Services on Wednesday, February 3, 2010. During the recovery process and internal investigation, AvMed determined that the data on the laptops was not properly secured. This means that protected health information of some current and

former members could be considered exposed. **Law enforcement is confident the laptops were stolen for their resale value, not with the intent of using the information on the laptops.**

What is AvMed doing to improve security?

AvMed has taken several steps to make its operations more secure and to eliminate future risk. Its Compliance Office is working to respond and make corrective actions according to state and federal regulations, including recently enacted HI-TECH laws and Florida Computer Crime laws.