

FBI Probes Hacker's \$10 Million Ransom Demand for Stolen Virginia Medical Records | Fox News

Published May 07, 2009

[FoxNews.com](http://www.foxnews.com)

0 0

The FBI is investigating a \$10 million ransom demand by a hacker or hackers who say they have stolen nearly 8.3 million patient records from a Virginia government Web site that tracks prescription drug abuse, an FBI official confirmed Wednesday.

The state police in Virginia are also investigating the possible breach of confidential records.

"This is a crime and it is being treated that way," Gov. Timothy M. Kaine said Wednesday.

The FBI official said the Virginia Information Technologies Agency (VITA) referred the case to the FBI last week, asking for help.

Asked whether people's personal information is secure, the official said he couldn't say.

"I really can't make a declarative statement as to whether anyone's information is in jeopardy at this point," the official said.

Asked whether people have been notified that their information may have been breached, the official said it would be up to VITA to do that.

The rogue government-transparency Web site WikiLeaks on Sunday [put up a message](#) that it said was posted Thursday on the front page of the Virginia Prescription Monitoring Program's Web site.

"ATTENTION VIRGINIA," the [message](#) read in part. "I have your [expletive]! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh :(

"For \$10 million, I will gladly send along the password. You have 7 days to decide. If by the end of 7 days, you decide not to pony up, I'll go ahead and put this baby out on the market and accept the highest bid."

The Virginia Prescription Monitoring Program's Web site, <http://www.pmp.dhp.virginia.gov/>, was offline Wednesday afternoon.

As Michael Fitzpatrick, president and CEO of the NCX Group, a Newport Beach, Calif.-based computer-security consulting firm, explained, "If the story wasn't true, the site would be back up."

Sandra Whitley Ryals, director of the Virginia Department of Health Professions, which runs the program, confirmed Wednesday that a criminal investigation is underway into the potential security breach on April 30.

"We can assure the public that all precautions are being taken for DHP operations to continue safely and securely," Ryals said in a statement.

Since the unauthorized message was posted, the department has been working "very closely and cooperatively with federal and state law enforcement to resolve the situation," she said.

"The entire DHP system has been shut down since Thursday to protect the security of the program data," Ryals said. "We are satisfied that all data was properly backed up and that these backup files have been secured."

The Department of Health Professions Web site had its own message: "The Virginia Department of Health Professions is currently experiencing technical difficulties which affect computer and email systems. We apologize for any inconvenience this may cause."

Laura Southerd, an official from the Virginia Department of Health, said the DOH is separate from the Department of Health Professions and uses different software to put up its Web site.

"The Prescription Monitoring Program Web site is now secure," she said. "But yes, something did happen."

Patient records could involve Social Security numbers, names and addresses — enough information for an identity-theft operation.

It's not clear how much 8 million patient records would fetch on the black market, but Fitzpatrick thought it'd be much more than \$10 million.

"That's a real 'Austin Powers' moment," he said. "That's \$1.20 per name. You could get a lot more for those in Griffiths Park in Los Angeles."

But even amateurs might have found the Prescription Monitoring Program Web site easy to get into, he added.

"Many government sites don't have the time or the money to fully check their code," Fitzpatrick explained. "And no offense, but the best security experts aren't going to work for \$60,000 for a state agency when they could make \$200,000 in the private sector."

There was no immediate reply to an e-mail sent to the address specified in the ransom note.

FoxNews' Bryan Boughton, Mike Levine, Mike Straka, Jennifer Lawinski and Paul Wagenseil contributed to this report.