

## VA investigating security breach of veterans' medical data

The [Veterans Affairs Department's](#) inspector general has launched a criminal investigation into a physician assistant's alleged downloading of veterans' clinical data at its Atlanta medical center, sources have told Nextgov.

The assistant allegedly recorded two sets of patient data on to a personal laptop for research purposes. One set included three years' worth of patient data and another held 18 years of medical information, according to a source familiar with the incident and who asked not to be identified.

[Roger Baker](#), VA's chief information officer, [commented](#) on an item about the incident that was posted Monday evening on a Nextgov blog that the physician assistant's laptop was never connected to the VA network and any data she recorded on her laptop was "hand entered."

But the source told Nextgov the VA inspector general is investigating whether the assistant used two thumb drives to transfer the data to the laptop.

The department has not disclosed the number of patients involved in the incident, what kind of personal data was copied, or whether it plans to notify the veterans whose records were downloaded.

VA spokeswoman Katie Roberts said she cannot comment in detail on the Atlanta breach because it is under investigation. But in an e-mail, she stated, "VA is committed to protecting the privacy of veterans who have used our health care facilities. VA's Office of Inspector General is currently investigating a report that a former VA physician assistant stored unauthorized clinical data about patients at the Atlanta [VA medical center] on a personal laptop computer.

"VA's Office of Information and Technology is trying to gather more details about the circumstances, including the number of veterans whose information was involved and the nature of the information affected. The results of the investigation and analysis will help determine whether to send notifications and offers of credit protection services to the affected veterans."

The inspector general has asked VA's Office of Information and Technology, which Baker heads, to determine how many veterans were involved in the data breach and what kinds of personally identifiable or private health information might be involved.

The inspector general has determined that multiple documents on the laptop "appear to have come from an unapproved research project," noted a document about the incident, which Nextgov obtained.

The incident is reminiscent of a 2006 [cybersecurity](#) breach at VA. In what was one of the largest security lapses in the department's history, a Veterans Affairs analyst [downloaded](#) information on 26.5 million patients -- practically every living veteran -- on to the hard drive of his personal laptop so he could work on a research project at home. The laptop was later stolen and recovered. Investigators determined the personal information likely was not accessed.

But the breach resulted in VA [instituting policies](#) to bar the connection of personal computers to Veterans Affairs networks and to encrypt all patient data stored on department computers. Violation of the policies could result in could result in administrative, civil or criminal penalties.

In his comment on the Nextgov blog, Baker said those policies worked in the Atlanta case and the physician assistant was denied access to VA systems. In addition, a nurse scientist and visiting scholar at the medical center stopped the assistant from using the data after learning about the unapproved research project, according to the document on the incident. The nurse told the physician assistant to destroy the data, and when it was not destroyed, the nurse informed a research compliance officer in Atlanta on Feb. 8. The physician assistant resigned on Feb. 26, according to the document.

The breach illustrates the need for patients, not clinicians, to control their medical records, said Dr. Deborah Peel, founder of Patient Privacy Rights, a nonprofit based in Austin, Texas, that works to ensure medical information remains restricted. She said control should include a requirement to obtain a patient's consent to send clinical information to another doctor or to use it for research. Peel added electronic consent software currently exists to automate the process