Audit finds slipshod cybersecurity at HealthCare.gov

September 25 2015, byRicardo Alonso-Zaldivar

In this Oct. 24, 2013 file photo, Andy Slavitt, now the acting Medicare administrator, testifies on Capitol Hill in Washington. A federal audit finds that the government stored sensitive personal information on millions of health insurance customers in a computer system with basic security flaws. The system is called MIDAS, the central electronic storehouse for information collected under President Barack Obama's health care law. (AP Photo/ Evan Vucci, File)

The government stored sensitive personal information on millions of health insurance customers in a computer system with basic security flaws, according to an official audit that uncovered slipshod practices.

The Obama administration said it acted quickly to fix all the problems identified by the Health and Human Services inspector general's office. But the episode raises questions about the government's ability to protect a vast new database at a time when cyberattacks are becoming bolder.

Known as MIDAS, the $110-million system is the central electronic storehouse for information collected under President Barack Obama's health care law.

It doesn't handle medical records. But according to a government privacy impact statement, it does include names, Social Security numbers, birthdates, addresses, phone numbers, passport numbers, employment status and financial account information of customers on HealthCare.gov and state insurance marketplaces.

"It sounds like a gold mine for ID thieves," said Jeremy Gillula, staff technologist for the Electronic Frontier Foundation, a civil liberties group focused on technology. "I'm kind of surprised that this information was never compromised."

The flaws uncovered by auditors included issues of security policy—where mistakes can have bigger consequences—as well as 135 database vulnerabilities, of which nearly two dozen were classified as potentially severe or catastrophic.

Among the policy mistakes: User sessions were not encrypted, contrary to standard practice on financial websites. "Not doing so is inexcusable

for such sensitive data," said Michelle De Mooy, deputy director for consumer privacy at the Center for Democracy & Technology, an Internet rights group.

MIDAS is an internal system operated by the federal Centers for Medicare and Medicaid Services, the agency that administers the health care law. The acronym stands for Multidimensional Insurance Data Analytics System. Officials say it's an electronic backbone, essential to the smooth operation of the health care law's insurance markets.

Currently about 10 million people are covered through HealthCare.gov and state marketplaces offering taxpayer-subsidized private policies. But MIDAS also keeps information on many others, including former customers. Their data is retained for years.

Before HealthCare.gov went live in 2013, Obama administration officials assured Congress and the public that individuals' information would be used mainly to determine eligibility for coverage, and that the government intended to store the minimum amount of personal data possible. Things don't seem to have turned out that way.

Among the technical problems uncovered by the audit:

—Using a shared read-only account for access to the database that contained individuals' personal information. Gillula said such a shared account creates a serious vulnerability because if data is stolen, it's much more difficult to tell who was looking at what information, and when.

—Failure to disable "generic accounts" used for maintenance or other special access during testing, an oversight that can foster complacency about security practices when a system becomes operational.

—Failure to conduct certain automated vulnerability scans that mimic

known cyberattacks and could reveal weaknesses in MIDAS and the systems supporting it.

—Database weaknesses. A total of 135 such vulnerabilities—oftentimes software bugs— were discovered by the inspector general's vulnerability scans. Of these, 22 were classified as high risk, meaning they could have potentially severe or catastrophic fallout, and 62 as medium risk.

"MIDAS collects, generates and stores a high volume of sensitive consumer information, and it is critical that it be properly secured," the inspector general's report reads. A summary omitting specific details of the vulnerabilities was posted on the IG's website this week.

In a written response to the audit, Medicare administrator Andy Slavitt said that "the privacy and security of consumers' personally identifiable information are a top priority" for his agency. Slavitt said all of the high vulnerabilities were addressed within a week of being identified, and that all of the IG's recommendations have been fully implemented.

The Medicare agency is conducting weekly vulnerability assessments of MIDAS, and an annual security review, Slavitt said.

However, the episode indicates how some technical and security issues from the program's chaotic rollout in 2013 may still linger. Back then, the consumer-facing side of HealthCare.gov went live without a completed security certification.

Gillula, the technology expert, said he doesn't question the administration's intentions. "I'm sure they wanted to do the right thing," he said. "But regardless of what they wanted, did they accomplish it? There certainly were some gaps."

More information: HHS Inspector General's

report—tinyurl.com/pycaesf

MIDAS privacy impact statement—tinyurl.com/nl79328