COSMOS
Navigate the Compliance Universe

# Report on Patient Privacy Volume 18, Number 8. August 31, 2018 Audit Finds Security Issues With Database Already Opposed by Plans Citing HIPAA

By HCCA Staff

The Office of Personnel Management (OPM) has been trying since 2010 to establish a health claims data warehouse (HCDW) to "better understand and control the drivers of health care costs" in the Federal Employees Health Benefits Program (FEHBP).

Referred to as the "largest employer-sponsored health insurance program in the country," some of the nation's biggest health plans, including Kaiser Permanente, Aetna, Humana, and Blue Cross plans, participate in the FEHBP. Collectively they enroll more than 8 million federal workers, retirees and their family members. But more than a year ago, they ceased sending information to the HCDW, citing security concerns and arguing that to forward OPM identifiable data as requested would be a HIPAA violation.

Now, a new audit by the Office of Inspector General (OIG) within OPM concludes the information technology "security controls" for the HCDW are "not in complete compliance with all standards." Among the issues: the HCDW has not had penetration testing and "has not been subject to routine continuous monitoring testing." Nor has OPM updated its contingency plan since it was written in 2015 when "the system was in development," OIG said in the audit.

The requirements that the HCDW must meet, including those developed by the National Institute of Standards and Technology (NIST), are mandatory for government agencies. But security experts recommend that HIPAA covered entities and business associates follow the NIST standards, making a review of the OIG findings instructive for them.

OIG made a dozen recommendations to shore up the HCDW; OPM effectively agreed to all of them. Despite the findings, OPM appears committed to moving ahead with the HCDW. Whether it can convince the plans to go along remains unknown. Confidence in OPM's ability to safeguard especially sensitive data has not been running high since the agency announced in 2015 that it had suffered a massive data breach, exposing information for some 20 million people.

According to OIG, standards applicable to the HCDW are those in the NIST Special Publication 800-53, in the Federal Information Security Modernization Act (FISMA), and in the Federal Information System Controls Audit Manual, as well as those set by OPM's Office of the Chief Information Officer.