E-BRIEF SERIES

Healthicity

February 2024 OIG Work Plan Updates

CJ Wolf MD, CHC, CPC, CCEP, CIA

The start of another month brings another review of new changes to the OIG's Work Plan. Here are a few key items for compliance professionals to review.

INFORMATION SECURITY (HHS GRANT PAYMENTS)

Information and data security is often on the minds of compliance officers. Data breaches are becoming more common, including those of government systems and/or their sub-contractors.

The OIG announced their intent to perform an audit of HHS' Program Support Center (PSC). PSC administers one of the Federal government's most widely used grant payment systems. Payment Management Services (PMS), a component of PSC, provides grant and grant-like payments, cash management, and grant accounting support services to HHS and other Federal departments and agencies.

There have been recent reports that $7.5 million has been stolen by hackers from HHS' grant payment system (see: https://www.bankinfosecurity.com/report-hackers-scammed-75m-from-hhs-grant-payment-system-a-24157 and https://www.bloomberg.com/news/articles/2024-01-18/us-health-department-cyber-attack-led-to-millions-in-grant-money-being-stolen?embedded-checkout=true).

Reportedly, access was obtained through a series of cyberattacks involving spear-phishing. The stolen funds were intended for rural communities and underserved patients. It was also reported that an HHS spokesperson said, "This matter has been referred to the OIG. As federal stewards of the taxpayer dollar, we take this issue with the utmost importance."

This is likely the impetus for this newly added OIG Work Plan item. The OIG states that PMS processes more than 70% of civilian grant payments made by the Federal government. The PMS expedites the flow of grant payments between the Federal government and grant recipients, provides grant recipient payment and expenditure data to awarding agencies, and helps manage cash advances to grant recipients.

OIG plans to gather information and conduct reviews of PSC and PMS relevant policies, procedures, and cybersecurity controls to determine whether the PMS was designed and is operating with effective controls.

Just as compliance programs need to ensure data security, the OIG expects that effective controls are established to prevent fraud and protect personally identifiable information (PII) from unauthorized access.

BACKGROUND CHECKS (LONG-TERM CARE PROVIDERS)

Most compliance professionals are aware of the background check activities performed by their organizations. They are important activities – and this is especially true for long-term care providers. Employees of long-term care providers are often caring for the most vulnerable patient populations among us. The Federal government, through the Centers for Medicare & Medicaid Services, has awarded more than $65 million to 28 states to design comprehensive national background check programs for direct patient access employees (for more information, see: https://www.cms.gov/medicare/enrollment-renewal/providers-suppliers/national-background-check).

The legislation that created the program also mandated that the OIG produce an evaluation of it within 180 days of the program's

completion. The OIG states that this Work Plan item report will be the final report in a series to fulfill this mandate. They hope to determine the extent to which States conducted background checks during and after program participation.

Additionally, OIG will determine:

- The cost of conducting background checks
- The number of applicants who received a background check
- Those who were disqualified from employment during and after NBCP participation
- Whether states experienced unintended consequences
- The program's impact on reducing the number of incidents of neglect, abuse, and misappropriation of resident property
- The long-term impact of the program

ALL OF US RESEARCH PROGRAM

The National Institutes of Health (NIH) oversees the All of Us Research Program (AoURP) which includes a research hub of data intended to match a broad research community with a diverse set of research participants.

Its goal is to advance precision medicine research and fuel new insights into human health. The Research Hub houses one of the largest, most diverse, and most broadly accessible datasets ever assembled (see: https://www.researchallofus.org/). It also provides an interactive Data Browser where anyone can learn about the type and quantity of data that AoURP collects. Users can explore aggregate data including genomic variants, survey responses, physical measurements, electronic health record information, and wearables data.

The AoURP is responsible for building a national research cohort of more than one million participants who provide their personal health information to NIH so that researchers, providers, and patients can work together to build a better future for health care. Individuals are less likely to share their data without the appropriate security and privacy controls to protect AoURP data. Institutions can register for access to the portal known as the "Researcher Workbench." The current list of registered institutions reads like a who's who of premier universities and research institutions (see: https://www.researchallofus.org/institutional-agreements/).

With the importance of data security in mind, the OIG has added this audit to its Work Plan. Their stated purpose is to determine whether the AoURP's award recipients:

1. Limit program research data access,
2. Implement information security and privacy controls, and
3. Remediate information security and privacy weaknesses in accordance with Federal requirements.

Prior OIG work identified inadequate controls in protecting participants' sensitive data for one of the two entities it audited (see: https://oig.hhs.gov/oas/reports/region18/181709304.asp).

Some of the findings included:

- Through penetration testing, OIG identified vulnerabilities that could have exposed the AoURP participants' PII, including their personal health information, and allowed unauthorized users to alter the participants' data.
- These vulnerabilities could have allowed an attacker with limited technical knowledge to exploit and compromise the PTSC's systems, as most of the vulnerabilities did not require significant technical knowledge to exploit.
- These vulnerabilities were not discovered before OIG's penetration testing because NIH did not adequately monitor the entity to ensure that it had implemented adequate cybersecurity controls to protect the participants' sensitive data.
- OIG identified several other issues that could affect the security of sensitive participant data. The entity failed to enable encryption in the S3 buckets.
- In addition, the entity did not have policies and procedures to address remediating source code vulnerabilities and timely disabling of network access.
- The entity did not adequately scan its network.

In contrast, the second entity the OIG audited appeared to have much better controls. About this second entity, the OIG stated they did not identify information system general control vulnerabilities. They attributed this positive finding to the entity's routine assessments and monitoring of its security controls. This "tale of two entities" can teach us a great deal about successful data security compliance programs.

The NIH responded to the OIG's initial work with the following statement: **https://allofus.nih.gov/news-events/announcements/statement-data-security-all-us-research-program**

The concluding sentence in the NIH's statement is: "Based on the OIG recommendation, we continue to review the security and privacy terms and conditions in our awards and will make any updates as needed to ensure we continue to have a multifaceted, robust security program." Perhaps this planned OIG audit will likely pressure test whether the NIH's oversight is truly working since the last OIG audit.

All of Us Research Program (AoURP) goal is to advance precision medicine research and fuel new insights into human health. The Research Hub houses one of the largest, most diverse, and most broadly accessible datasets ever assembled.

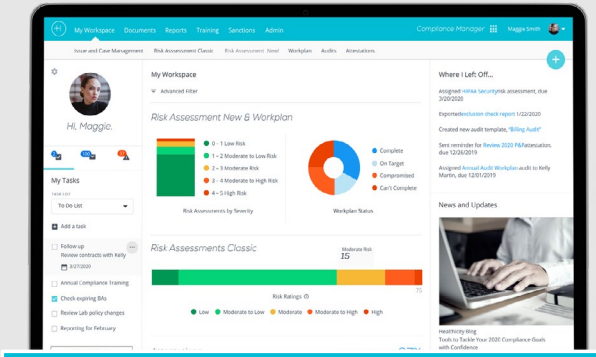
CJ Wolf

MD, CHC, CPC, CCEP, CIA

CJ Wolf is a healthcare professional with more than 20 years of experience in hospital and physician revenue cycle, practice management, compliance, coding, billing, and client services. He has provided healthcare consulting and solution services to hospitals and physician organizations throughout the country.

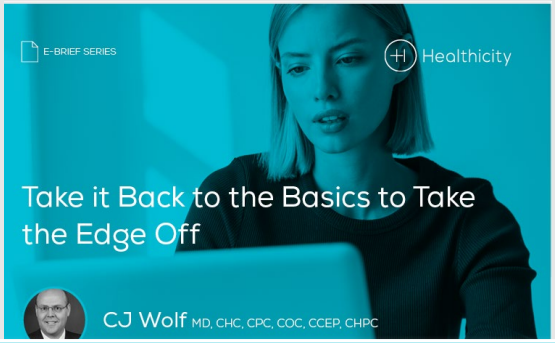
For more on Healthicity's Compliance Services and Solutions, please visit healthicity.com/compliance or call 877.777.3001

COMPLIANCE MANAGER



WATCH ON-DEMAND DEMO

RESOURCE CENTER



EXPLORE FREE RESOURCES