Health Information Compliance Alert

Compliance: Telemedicine, EHR Fraud Factor in New OIG Report

Tip: Use the feds' targets as a compliance guide.

If you're waiting for federal fraud-fighting efforts to lighten up, you'll be waiting a long time. And in its latest iteration, the **U.S. Department of Health and Human Services Office of Inspector General** (OIG) puts emphasis on health IT fraud and abuse.

Here Are the Numbers

In its latest Semiannual Report to Congress, which covers OIG activity for the reporting period that runs from October 1, 2018 to March 31, 2019, the federal watchdog expects to recover $496 million from audits and $2.3 billion from investigations. Other numbers from this first part of the 2019 fiscal year include:

- **Civil actions:** OIG instigated civil actions against 331 individuals, including monetary penalties.
- **Criminal actions:** The feds initiated criminal charges against 421 individuals.
- **Exclusions:** 1,293 individuals found themselves excluded from federal healthcare programs.

"OIG continues building its capabilities to harness emerging technologies in its oversight of Department programs," says former Inspector General **Daniel R. Levinson** in the report's introduction. "For example, OIG's multidisciplinary cybersecurity team helps the Department prevent and combat cyber threats by fostering enhancements in information technology controls, risk management, and resiliency."

Levinson mentions the agency's focus on protecting scientific data at the **National Institutes of Health** (NIH) and its recommendation that the **Food and Drug Administration** (FDA) strengthen mandates on medical devices to make them less pliable for hackers. He adds, "Moving forward, OIG will continue to modernize technology infrastructure, develop new data analytic tools, and explore emerging areas such as artificial intelligence and machine learning."

In addition to looking at the agency's biggest takedowns, target areas, and commitment to protecting beneficiaries, the report also notes Levinson's departure as OIG's chief.

See 3 Health IT-Related Cases

The OIG's Semiannual Report offers advice, insight, and cost-saving measures to HHS on ways to improve the various federal healthcare programs and departments that fall under its umbrella; however, a big chunk of the brief focuses on fraud across the healthcare spectrum. Investigations include cases that involve patient abuse; "billing for services not rendered, medically unnecessary services, or upcoded services;" the myriad of prescription drug offenses; and kickbacks and referral schemes, the report indicates.

The following three cases were among the OIG's reported triumphs over the six-month period that relate specifically to health IT, according to the report:

- **Telemedicine scheme:** "Operation Brace Yourself" was one of the federal watchdog's major takedowns during this fiscal period. "OIG and law enforcement partners dismantled one of the largest healthcare fraud schemes ever investigated, involving allegations of almost $1 billion paid for medically unnecessary orthopedic braces furnished through a telemarketing scam to seniors," the report says. Twenty-four defendants were charged, including three medical professionals and five telemedicine firms. The cases are still in the prosecution stage across several federal jurisdictions.
- **Shoddy software:** Electronic health record (EHR) company, **eClinicalWorks LLC** (ECW), finalized its corporate integrity agreement (CIA). Back in 2017, ECW agreed to pay the feds $155 million for false claims

under the False Claims Act (FCA) for concealing "from its customers that its software did not comply with the requirements for 'meaningful use' certification," the report notes. The CIA requires the EHR firm to hire an "Independent Software Quality Oversight Organization" to scrutinize its practices and protect patients, adds the OIG.

- **EHR kickbacks:** Health IT software company, **Greenway Health LLC,** consented to an FCA settlement, agreeing to pay $57.25 million, the report indicates. Plus, the organization will enter into a five-year CIA with OIG. The settlement, fines, and CIA resolve the "FCA liability" that includes misrepresenting **HHS Office of the National Coordinator for Health Information Technology** (ONC) certification of its software "Prime Suite," OIG says. The software didn't comply with the certification and instead caused providers to falsely attest under the Meaningful Use program. The company also incentivized some providers to use the slipshod software against the rules of the Anti-Kickback Statute (AKS).

How Does This Impact You?

Practices concerned about navigating the choppy waters of compliance can learn a lot about the government's fraud and abuse targets from the feds briefs. Moreover, the information you garner from perusing the daily actions, monthly work plans, semiannual reports, and annual reviews can help you devise a plan to steer clear of the OIG's spotlight. Plus the reviewed cases highlight the importance of vetting your vendors and checking into the background of your business associates (BAs).

"The OIG's semiannual reports indicate the current areas of concern for the OIG," explains Jackson, Mississippi-based attorney **Jonell B. Beeler,** with national firm **Baker Donelson** in its Health Law Alert blog. "Healthcare providers can utilize the insight offered by the report to review their own practices as they relate to the OIG's investigative focus issues and thereby ensure they are not on a path to becoming a statistic on the next report."

Read the Semiannual Report to Congress at
https://oig.hhs.gov/reports-and-publications/archives/semiannual/2019/2019-spring-sar.pdf.