Part B Insider (Multispecialty) Coding Alert

Physician Notes: CMS' Analytics System Caught $820 Million in Fraud

Plus: Hospital settles for $218,400 over HIPAA violation.

CMS uses many approaches to catching fraud, and its high-tech analytics system is one of the most lucrative tools for the agency. On July 14, CMS announced that its Fraud Prevention System identified or prevented $820 million in inappropriate payments over a three-year period, with $454 million of that amount in just 2014 alone.

The system uses analytics software to identify questionable billing patterns among Medicare claim submissions. "In one case, one of the system's predictive models identified a questionable billing pattern at a provider for podiatry services that resulted in Medicare revoking the provider's payments and referring the findings to law enforcement," CMS said in the news release announcing the savings. CMS hopes to expand the Fraud Prevention system algorithms to lower-levels of compliance among healthcare providers who need education on claims submissions.

"We are proving that in a modern health care system you can both fight fraud and avoid creating hassles for the vast majority of physicians who simply want to get paid for services rendered. The key is data," said CMS Acting Administrator **Andy Slavitt** in a statement. "Very few investments have a 10:1 return on taxpayer money."

In other news...

A Massachusetts hospital owes the government $218,400 after being charged with HIPAA violations over the last three years, and must create a corrective action plan to ensure it doesn't happen again.

The settlement comes after a 2012 complaint alleging that the hospital used an online document sharing app to store data that included protected health information (PHI), despite the risks that it posed. In addition, the hospital also faced scrutiny in 2014 after unsecured PHI was found on a former employee's laptop and flash drive. The data impacted 595 different patients.

"Organizations must pay particular attention to HIPAA's requirements when using internet-based document sharing applications," said OCR Director **Jocelyn Samuels** in a July 10 statement. "In order to reduce potential risks and vulnerabilities, all workforce members must follow all policies and procedures, and entities must ensure that incidents are reported and mitigated in a timely manner."

Resource: To read more about the settlement, visit www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/SEMC/bulletin.pdf.