Health Information Compliance Alert

Patient Privacy: More Reasons For You To Thwart Patient Privacy Breaches

OIG finds even CMS fallible.

Have you ever wondered how the **Centers for Medicare & Medicaid Services** keep all 40+ million Medicare beneficiaries protected under HIPAA? Keeping the privacy secure for the patient base of a practice or a facility is challenging enough. The troubling truth is that the agency is subject to the same penalties that you are in the event of a breach -- and it is also vulnerable to privacy breaches.

Between 2009 and 2011, CMS reported that it had 14 breaches of protected health information (PHI) requiring notification to the 13,775 Medicare beneficiaries affected, according to the OIG report, "CMS Response to Breaches and Medical Identity Theft," released on Oct. 10.

Background: The Recovery Act requires covered entities to notify any individual whose PHI has been breached. If a breach impacts 500 or more residents of a state or jurisdiction, the entity must also notify media outlets in the area to distribute the word of the PHI leak.

The OIG sought to determine whether CMS responded appropriately to any PHI breaches that the agency or its contractors caused between Sept. 23, 2009 (when the Recovery Act went into effect) and Dec. 31, 2011.

One Mailing Error Impacts 13,412 Patients

CMS self-identified 14 breaches over the review period, impacting 13,775 beneficiaries total. However, one breach constituted the majority of the issues, affecting 13,412 patients. In that instance, a contractor erroneously sent Medicare Summary Notices containing PHI to the wrong addresses.

Ten additional breaches were attributed to mis-mailings or loss of documents during transit, while another two breaches involved beneficiary information being posted online. The final breach was discovered when a CMS contractor employee was arrested for stealing beneficiary information.

The OIG found that CMS appropriately notified all beneficiaries impacted by the 14 breaches, but did not meet the timeliness standard in seven instances. The Recovery Act dictates that breach notifications should be sent to beneficiaries within 60 days of discovery, but CMS took up to four months longer than that in a few cases, the OIG reports.

In response to the report, CMS noted that it "will develop new procedures and/or modify existing ones to improve the breach notification process."

Resource: To read the complete OIG report, visit https://oig.hhs.gov/oei/reports/oei-02-10-00040.pdf.