

Feds to track how private Medicare info gets to marketers

February 14 2020, by Ricardo Alonso-Zaldivar



The Official U.S. Government Medicare Handbook for 2020 over pages of a Department of Health and Human Services, Office of the Inspector General report, are shown, Thursday, Feb. 13, 2020 in Washington. A government watchdog tells The Associated Press it will launch a nationwide audit that may shed light on how seniors' personal Medicare information is getting to telemarketers, raising concerns about fraud and waste. An official with the Health and Human Services inspector general's office says the audit will be announced next week. (AP Photos/Wayne Partlow)

A government watchdog plans to launch a nationwide probe into how telemarketers may be getting hold of seniors' personal Medicare information, a red flag for potential fraud and waste.

An official with the Health and Human Services inspector general's office told The Associated Press the audit will be announced next week. It would follow a narrower probe which found that an electronic system designed for pharmacies to verify Medicare coverage was being used for searches that appeared to have nothing to do with filling prescriptions. The official spoke on condition of anonymity ahead of a formal announcement.

The watchdog agency's decision comes amid a wave of relentlessly efficient telemarketing scams targeting Medicare recipients and involving everything from back braces to DNA cheek swabs.

For years, seniors have been admonished not to give out their Medicare information to people they don't know. But a report on the initial probe, provided to the AP, details how sensitive details can still get to telemarketers when a Medicare beneficiary thinks he or she is dealing with a trustworthy entity such as a [pharmacy](#) or doctor's office.

Key [personal details](#) gleaned from Medicare's files can then be cross-referenced with databases of individual phone numbers, allowing marketers to home in with their calls. The report is being released Friday.

The initial audit focused on 30 pharmacies and other service providers that were frequently pinging a Medicare system created for drugstores.

The [electronic system](#) is intended to be used for verifying a senior's

eligibility at the sales counter. It can validate coverage and personal details on millions of individuals. Analyzing records that covered 2013-15, investigators discovered that most of the audited pharmacies, along with a [software company](#) and a drug compounding service also scrutinized, weren't necessarily filling prescriptions.

Instead, they appeared to have been tapping into the system for potentially inappropriate marketing.

Medicare stipulates that the electronic queries—termed "E1 transactions"—are supposed to be used to bill for prescriptions. But investigators found that some pharmacies submitted tens of thousands of queries that could not be matched to prescriptions. In one case, a pharmacy submitted 181,963 such queries but only 41 could be linked to prescriptions.

The report found that on average 98% of the electronic queries from 25 service providers in the initial audit "were not associated with a prescription." The inspector general's office did not identify the pharmacies and service providers.

Pharmacies are able to access coverage data on Medicare recipients by using a special provider number from the government.

But investigators found that four of the pharmacies they audited allowed marketing companies to use their provider numbers to ping Medicare. "This practice of granting telemarketers access to E1 transactions, or using E1 transactions for marketing purposes puts the privacy of the beneficiaries' (personal information) at risk," the report said.

Some pharmacies also used seniors' information to contact doctors treating those beneficiaries to see if they would write prescriptions. Citing an example, the report said, "The doctor often informed (one)

provider that the beneficiary did not need the medication."

The inspector general's office said it is investigating several [health care providers](#) for alleged fraud involving E1 transactions. Inappropriate use of Medicare's eligibility system is probably just one of many little-known paths through which telemarketers can get sensitive personal information about beneficiaries, investigators said.

The watchdog agency began looking into the matter after the Centers for Medicare and Medicaid Services, or CMS, asked for an audit of a mail order pharmacy's use of Medicare's eligibility verification system.

In a formal response to the report, CMS Administrator Seema Verma said CMS retooled its verification system last year so it automatically kicks out queries that aren't coming from a pharmacy. More than a quarter-million such requests have been rejected, she wrote.

Medicare is committed to ensuring that the system is used appropriately, Verma added. The agency can revoke access for pharmacies that misuse the privilege and is exploring other enforcement options.

The inspector general's office acknowledged Medicare's countermeasures but said it wants to see how effective they've been.

Health care fraud is a pervasive problem that costs taxpayers tens of billions of dollars a year. Its true extent is unknown, and some cases involve gray areas of complex payment policies.

In recent years, Medicare has gotten more sophisticated, adapting techniques used by financial companies to try to head off fraud. Law enforcement coordination has grown, with strike forces of federal prosecutors and agents, along with state counterparts, specializing in health care investigations.

Officials gave no timetable for completing the audit.

© 2020 The Associated Press. All rights reserved.

Citation: Feds to track how private Medicare info gets to marketers (2020, February 14)
retrieved 24 April 2024 from

<https://medicalxpress.com/news/2020-02-feds-track-private-medicare-info.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.