CLIENT ALERTS & INSIGHTS

OIG and DOJ Intensify Remote Patient Monitoring Oversight: 2025 Data Snapshot, FCA Settlement and the Emerging Enforcement Playbook

OCTOBER 10, 2025

Authors: Nesko Radovic, Scott P. Downing, Jason S. Greis, Jake A. Cilek, Christopher DeGrande, Daniel Meier, Kathrin “Kat” Zaki

Key Takeaways

- Federal oversight of Remote Patient Monitoring (“RPM”) is increasing, as agencies like the OIG, CMS and DOJ shift from issuing warnings to actively enforcing regulations. This includes standardized audit metrics and the first False Claims Act (“FCA”) settlement related to RPM billing.
- The risk of audits, investigations and significant financial penalties is now much higher for RPM stakeholders. The government is using data-driven audit triggers and has already demonstrated willingness to pursue FCA actions for non-compliance, making even technical or documentation errors a potential source of liability.
- Providers and RPM vendors can prepare by reviewing and strengthening their compliance programs: tracking OIG-identified risk patterns, ensuring thorough documentation of patient-provider relationships, verifying that treatment management is substantive, and carefully vetting vendor practices. Proactive compliance and internal audits are essential to mitigate enforcement risk before audits and investigations escalate.

Federal oversight of Remote Patient Monitoring ("RPM") has entered a new and more aggressive phase. In less than two years, the Office of Inspector General ("OIG"), the Centers for Medicare & Medicaid Services ("CMS"), and the Department of Justice ("DOJ") have advanced from initial public warnings about fraudulent RPM schemes to a coordinated enforcement posture built on structured oversight recommendations, standardized audit metrics and the first False Claims Act ("FCA") settlement involving RPM billing practices.

In parallel with these enforcement developments, CMS is also reshaping the underlying billing and reimbursement framework for RPM and Remote Therapeutic Monitoring ("RTM"). As we addressed in our prior alert on CMS's proposed 2025 RPM/RTM rule changes, the agency has proposed significant policy updates that will affect coding, billing frequency and patient eligibility requirements. These parallel regulatory and enforcement tracks-rulemaking on one hand and audit standardization and enforcement on the other-are converging, underscoring that RPM compliance now involves both prospective alignment with new billing rules and retrospective scrutiny of existing billing practices

The August 2025 OIG Data Snapshot on RPM billing practices is particularly significant. It signals that the federal government is no longer simply observing RPM utilization growth; it is actively setting the audit playbook that CMS contractors and Medicare Advantage plans will use going forward. The DOJ settlement announced two months earlier confirms that billing misconduct in this area carries real enforcement consequences.

Together, these actions reflect a deliberate regulatory trajectory that mirrors OIG's approach to other high-growth, high-risk billing areas such as telehealth and DMEPOS. This alert reviews these developments in detail and outlines practical implications for RPM stakeholders.

I. OIG's August 2025 Data Snapshot: Standardizing RPM Audit Indicators

On August 25, 2025, OIG released its Data Snapshot, "Billing for Remote Patient Monitoring in Medicare" (OEI-02-23-00261). This publication provides a data-driven framework for identifying RPM billing outliers, based on 2024 Medicare fee-for-service and Medicare Advantage encounter data.

The Data Snapshot reveals that RPM utilization continued to expand rapidly in 2024: nearly one million Medicare beneficiaries received RPM services, and total payments climbed to approximately $536 million, a 31 percent increase over the prior year. Approximately 4,600 medical practices met OIG's threshold for "routinely billing RPM," defined as enrolling at least 10 patients and submitting at least 100 RPM claims during the year.

Within this population, OIG identified five billing patterns warranting heightened scrutiny:

- **Abrupt and disproportionate spikes in patient enrollment.** OIG highlighted practices showing sudden enrollment growth of 150% or more month-over-month, including one that billed for roughly 3,400 new RPM patients in a single month.
- **Billing without documented prior patient-provider relationships.** Forty-five practices billed RPM for over 80% of their patients without any prior in-person or telehealth encounter, despite CMS reinstating this requirement after the COVID-19 Public Health Emergency ("PHE").

- **Extended periods of device billing without treatment management.** Fifty-two practices billed device codes month after month without corresponding monthly management services for more than 75% of patients.
- **Multiple providers billing for the same beneficiary.** OIG found 34 practices with overlapping claims, raising duplication and medical necessity concerns.
- **Multiple devices billed for the same patient in a single month.** Roughly 20 practices consistently billed for two or more devices per beneficiary per month, far outside Medicare norms.

OIG was careful to emphasize that these patterns are not per se evidence of fraud. Instead, they are screening metrics designed to help CMS contractors, Medicare Advantage plans and OIG itself prioritize program integrity reviews. Once OIG publishes metrics like these, they typically become embedded in contractor audit algorithms-just as similar telehealth metrics did during and after the COVID-19 PHE.

II. DOJ's June 2025 FCA Settlement: Enforcement Arrives

Two months earlier, DOJ demonstrated how RPM billing failures can result in FCA liability. On June 26, 2025, the U.S. Attorney's Office for the Northern District of Georgia announced a $1.29 million FCA settlement with Health Wealth Safe, Inc. and its owner, Dr. Subodh Agrawal.

The government alleged that, between 2019 and 2021, the defendants billed Medicare for RPM services without furnishing devices capable of automatically collecting and transmitting patient data, a basic coverage requirement. The case originated as a qui tam action; OIG participated in the investigation.

Although the alleged conduct predated OIG's Data Snapshot, the underlying issues-technical device noncompliance, lack of verifiable monitoring activity and billing for non-qualifying services-align closely with the billing patterns OIG has now flagged. This settlement demonstrates DOJ's willingness to treat RPM billing misconduct as a false claims risk, not merely a compliance issue, and underscores that enforcement is already underway.

III. OIG's September 2024 Oversight Report: Diagnosing Structural Vulnerabilities

The September 2024 OIG evaluation report, "Additional Oversight of Remote Patient Monitoring in Medicare Is Needed" (OEI-02-23-00260), set the stage for the subsequent metric-setting and enforcement actions.

OIG documented the tenfold growth in RPM utilization between 2019 and 2022 and a corresponding increase in payments from $15 million to more than $300 million. It also identified serious compliance gaps. Most notably, 43% of beneficiaries receiving RPM during that period did not receive all three required service components-patient education and setup, device supply, and monthly treatment management-indicating widespread incomplete or improper billing.

OIG further found that CMS lacked meaningful insight into the types of devices being used, the data collected and who ordered the services, and that CMS had no systematic mechanism to identify RPM-specialist companies. These weaknesses limited CMS's ability to conduct targeted oversight.

In response, OIG issued five key recommendations to CMS:

- Implement new safeguards to address inappropriate or excessive billing;
- Require ordering provider identifiers on claims to enhance traceability;
- Collect more detailed device and data information to allow for targeted oversight;
- Provide enhanced provider education to clarify coverage and documentation expectations; and
- Develop methods to identify and monitor RPM-specialist entities, similar to DME supplier tracking.

CMS concurred with or agreed to consider all of these recommendations. In regulatory terms, this was the oversight recommendation stage, in which OIG formally diagnosed program vulnerabilities and CMS committed to addressing them. This stage typically provides the analytical and policy foundation for later audit standardization and enforcement.

IV. OIG's November 2023 Consumer Alert: Early Identification of Fraud Patterns

The trajectory began in November 2023, when OIG issued a Consumer Alert warning Medicare beneficiaries about fraudulent RPM enrollment schemes. These schemes involved aggressive marketing through cold calls and online ads, enrollment without legitimate clinical justification, provision of non-compliant or nonexistent devices, and billing for phantom monitoring.

Although directed at beneficiaries, this alert revealed that OIG had already identified organized RPM scam structures and was attempting to curb their expansion. Many of the fraudulent behaviors described here would later be codified as billing risk indicators in the 2025 Data Snapshot.

V. Enforcement Trajectory: From Observation to Standardization

Taken together, the 2023 Consumer Alert, 2024 oversight report, 2025 Data Snapshot and 2025 FCA settlement represent a deliberate regulatory progression. OIG began by observing and publicizing fraudulent practices, moved to analyzing structural weaknesses and making policy recommendations, then standardized empirical audit triggers, and finally initiated enforcement actions through DOJ.

This pattern-observation → oversight recommendations → metric-setting → enforcement-is a familiar one. It mirrors how OIG and CMS addressed telehealth during and after the PHE: identify scam patterns, study vulnerabilities, set data-driven audit criteria and then launch targeted reviews and FCA actions. RPM is now following that same trajectory and the government is firmly in the enforcement phase.

VI. Practical Implications for Providers and RPM Vendors

For physician groups, other providers and RPM vendors, these developments have immediate and significant compliance implications:

- **Integrate OIG's risk patterns into internal monitoring.** Compliance programs should track the five billing patterns identified in the 2025 Snapshot-enrollment spikes, prior relationship documentation, treatment management activity, multiple providers and multiple devices-as internal triggers. Outliers should be explainable and well-documented.
- **Document patient-provider relationships meticulously.** The reinstated requirement for a prior encounter is now a focal point for OIG and CMS; gaps in encounter documentation are likely to draw scrutiny.
- **Ensure treatment management is substantive and timely.** Long stretches of device billing without management are explicitly identified as audit red flags. Providers should be able to demonstrate meaningful clinical engagement with RPM data.
- **Vet vendors carefully.** Contracts should address device transmission standards, marketing practices and data handling. Providers remain legally responsible even when vendors manage logistics.
- **Prepare for multidimensional enforcement risk.** OIG's audit metrics will inform contractor reviews; CMS policy changes will shape reimbursement rules; and DOJ's use of the FCA will magnify financial exposure. Proactive compliance-before widespread audits begin-is both strategically and financially critical.

VII. Conclusion

RPM has evolved from a promising care management tool into a major focus of federal program integrity oversight. The consumer alert, oversight report, data snapshot and DOJ settlement trace a clear and deliberate enforcement arc. OIG has identified fraudulent behaviors, mapped structural vulnerabilities, standardized audit metrics and demonstrated that enforcement will follow.

Providers and vendors should not view these developments as background noise. They are a regulatory roadmap for the next phase of RPM oversight. Those who act now to align their operations, documentation and compliance protocols with OIG's expectations will be better positioned to withstand the coming wave of audits and enforcement.

Benesch Healthcare+ will continue to monitor OIG, CMS and DOJ developments in RPM and RTM. Our team regularly advises providers, physician groups and technology partners on structuring compliance programs, conducting proactive audits and responding to enforcement inquiries in this rapidly evolving regulatory landscape.

For further information, please contact the authors of this article or any member of the Benesch Healthcare+ team.