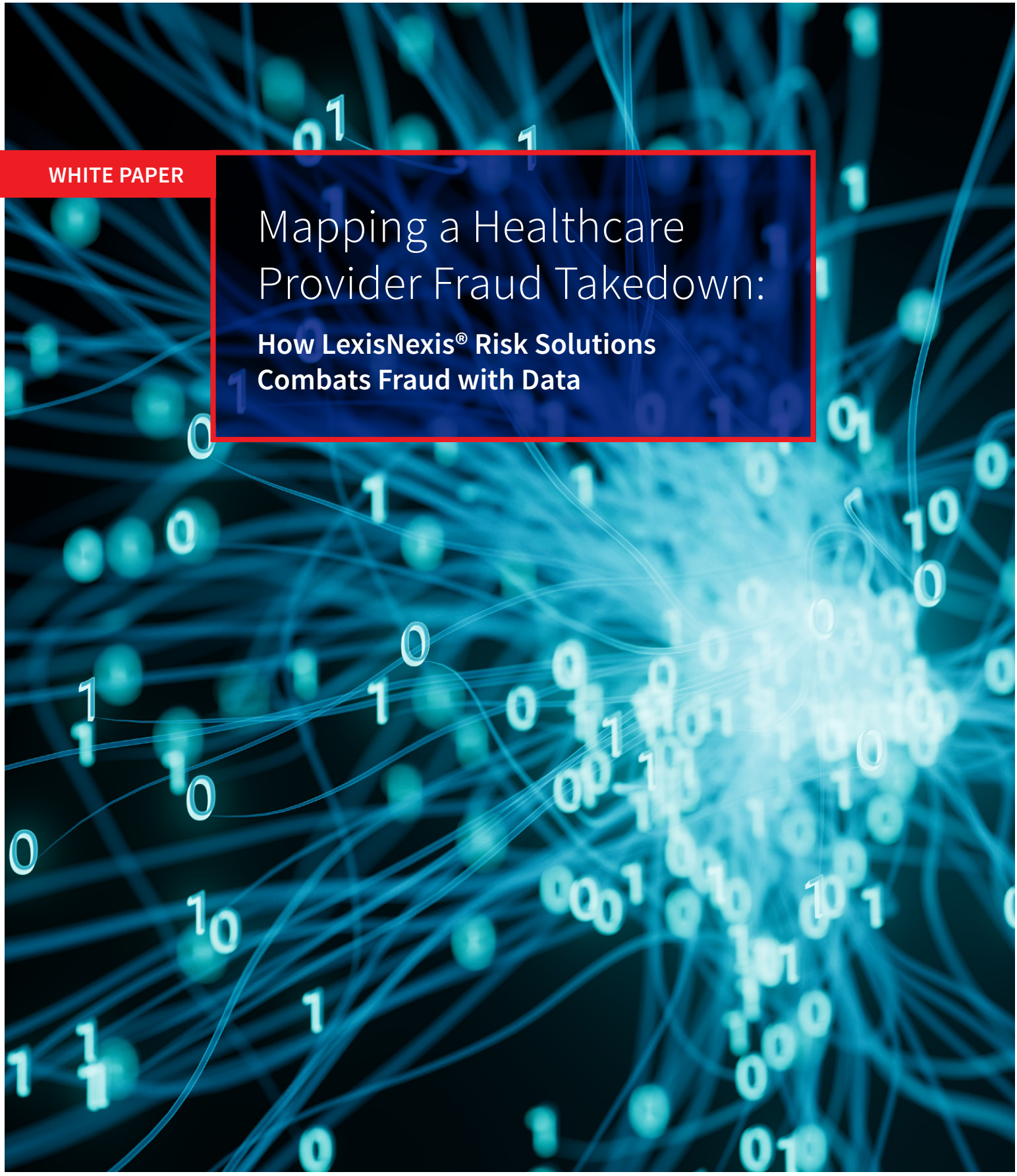
LexisNexis®
RISK SOLUTIONS



WHITE PAPER

Mapping a Healthcare Provider Fraud Takedown:

How LexisNexis® Risk Solutions Combats Fraud with Data

WHITE PAPER

Medicare and Medicaid fraud remains one of the most pervasive threats to the integrity of U.S. healthcare programs. Since their creation in 1965, Medicare and Medicaid have ensured that older adults, people with disabilities, and individuals and families with limited incomes can receive the care, dignity, and support they deserve when accessing essential health services.

But alongside its successes, these programs have faced a persistent shadow: fraud. From their earliest days, criminals have sought to exploit Medicare and Medicaid's vast resources, creating one of the most enduring challenges in U.S. healthcare.

Recent enforcement actions have shown how bad actors, often foreign criminal networks, exploit vulnerabilities across fragmented systems, siphoning billions in taxpayer funds.

The scale and sophistication of these schemes highlight an urgent need for an identity-driven approach to fraud detection and prevention.

WHITE PAPER

The Growing Fraud Challenge

The growing fraud challenge facing Government healthcare programs is vast and increasingly complex. In the Justice Department's 2025 Healthcare Fraud Takedown, more than 320 individuals were charged in schemes involving over $14.6 billion in intended loss, highlighting the massive scale of this fraud. 96 of these individuals were licensed medical professionals, underscoring the importance of understanding providers who interact with government programs, including Medicare and Medicaid.

Operation Gold Rush was the centerpiece of the 2025 National Health Care Fraud takedown, exposing a transnational criminal network that exploited Medicare through stolen identities and fraudulent billing schemes accounting for over $10.6 billion in false claims.[1] By illicitly purchasing dozens of durable medical equipment (DME) companies already enrolled in Medicare, this criminal network submitted fraudulent claims using stolen identities of more than one million Americans, many of whom were elderly or disabled. They successfully collected nearly $1 billion before detection.

In addition to intentional fraud perpetrated by bad actors, well-intentioned policies are also being exploited in ways that distort funding flows and compromise care to Medicare beneficiaries that need it most. A December 2022 GAO report revealed that **Centers for Medicare & Medicaid Services (CMS) waived critical safeguards during the COVID-19 emergency, allowing over 220,000 providers to enroll without fingerprint checks or site visits—many of whom were later deemed ineligible.**[3] An April 2024 GAO report underscored the ongoing need to revalidate enrollment for Medicare providers after the COVID-19 pandemic.[4]

In Los Angeles, investigators uncovered **widespread hospice fraud, identifying more than 1,000 potentially fraudulent hospice providers**, many operating as little more than mailing-address fronts, billing Medicare for services never delivered.[2]

These examples highlight the urgent need for more robust screening, oversight, and data integrity across Medicare's provider infrastructure. Policy loopholes and enrollment system gaps are distorting Medicare's resource allocation and compromising program integrity.

As fraudsters become increasingly sophisticated, integrating advanced identity management and risk analytics is no longer optional—it's essential for protecting patient data, preserving trust, and ensuring the integrity of care delivery.

WHITE PAPER

The Core Problem: Siloed and Outdated Provider Data

CMS plays a critical role in safeguarding the integrity of federal healthcare programs. To oversee its vast network of providers, CMS relies on several systems—National Plan and Provider Enumeration System (NPPES), Provider Enrollment, Chain, and Ownership System (PECOS), and Automated Provider Screening (APS). While each was designed with a specific purpose, they share a common limitation: they capture partial and often outdated snapshots of provider information and rely heavily on self-reported data.

The problem lies not just in the data itself, but in how these systems operate. Each functions in a silo, with little to no integration across platforms. This fragmented structure prevents CMS from building a comprehensive view of providers. It also creates significant blind spots when it comes to tracking ownership changes, monitoring affiliations, or identifying operational shifts in real time.

Without a dynamic risk profile of providers, enforcement efforts lag far behind fraudulent activity. Individuals with prior convictions, shell companies, and straw ownership schemes exploit these gaps, escaping CMS oversight. In many cases, such bad actors remain in the system for years, billing taxpayer-funded programs until enforcement finally catches up—often long after the damage has been done.

A March 2025 HHS OIG report exposed how weak identity verification protocols allowed fraudsters to impersonate providers and divert Medicare payments by changing payment information stored in systems such as PECOS.[5] Given how widely electronic funds transfer transactions are used in health care transactions, the risk for large losses due to poor provider data is immense.

WHITE PAPER

The stakes are high. Fraudulent providers not only drain billions from Medicare, but also put patients at risk by compromising the quality of care. To address these vulnerabilities, CMS must move toward a modernized, integrated oversight framework. That means breaking down data silos, enabling real-time monitoring, and building dynamic provider risk profiles that can adapt as ownership and operational changes occur.

To close these gaps, CMS must establish a **single source of truth** for provider identity and risk that relies on both traditional and non-traditional data sets to ensure a comprehensive understanding of a provider and the entities that they are associated with. In doing so, they can:

- **Reconcile and clean data** across all systems.
- **Verify identity and ownership structures**, including hidden affiliations and control.
- **Ensure operational status accuracy** so terminated or excluded providers cannot re-enter under new guises.

The Paradigm Shift: A Provider-Centric, Integrated System

A sustainable solution requires more than patchwork fixes. CMS needs a provider-centric, integrated risk management platform that continuously monitors provider status from enrollment to exit, detects and surfaces real-time changes in ownership, affiliations, or suspicious activity, and maintains an active, dynamic risk profile for every provider.

By consolidating overlapping systems into a streamlined, coordinated environment, CMS can reduce redundancy while strengthening oversight. This transformation would enable the agency to flag suspicious entities early—before fraudulent claims are paid—and remove bad actors swiftly, protecting both program integrity and taxpayer dollars.

WHITE PAPER

Where LexisNexis Risk Solutions Fits

CMS faces an ongoing challenge: how to effectively monitor a vast and complex network of healthcare providers whose underlying data is always changing, while preventing fraud, waste, and abuse. Fragmented systems, outdated data, and limited real-time monitoring have left critical gaps in oversight. Addressing this challenge requires not just incremental fixes, but a comprehensive, data-driven approach—and this is where LexisNexis Risk Solutions comes in.

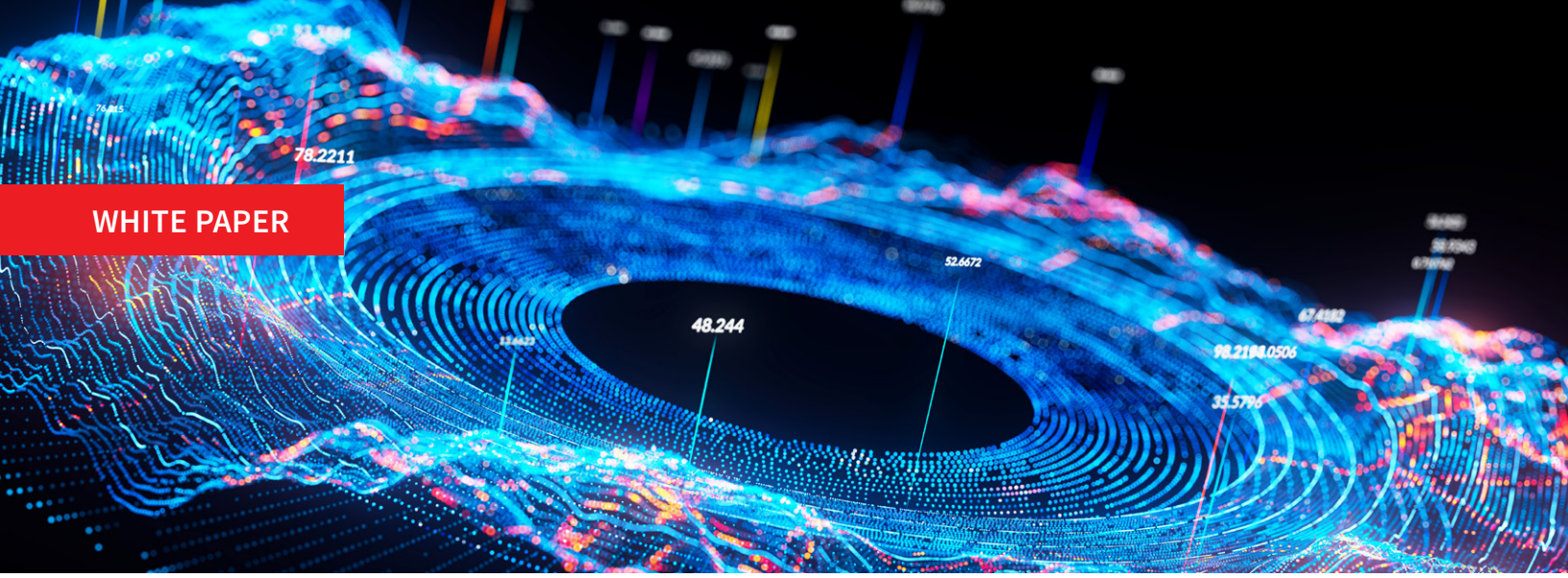
With decades of **expertise in identity verification, risk analytics, and data integration**, LexisNexis offers capabilities directly aligned to CMS' needs. Through advanced entity resolution and identity intelligence, the company reconciles billions of public and proprietary records to create comprehensive and up-to-date views of providers.

LexisNexis® Risk Solutions **affiliation and ownership analytics** take this a step further. By leveraging sophisticated linkage technology, LexisNexis Risk Solutions can identify hidden relationships between providers, facilities, and networks of fraud, waste, and abuse. These insights allow CMS to identify complex schemes that traditional oversight tools might miss.

Real-time monitoring adds yet another layer of protection. Continuous data feeds track changes in provider status, ownership, or location, surfacing risk the moment it emerges. This proactive approach allows CMS to intervene early, before fraudulent claims are submitted and taxpayer dollars are lost.

Finally, LexisNexis® Risk Solutions **data integration and cleaning capabilities** create a single source of truth. Fragmented records from multiple systems can be consolidated into a unified, provider-centric platform, reducing redundancy and improving efficiency while supporting more informed decision-making.

In an era of increasingly sophisticated healthcare fraud, CMS requires more than patchwork solutions. By leveraging the tools and expertise of LexisNexis Risk Solutions, CMS can modernize provider oversight, detect risk in real time, and protect the integrity of critical healthcare programs—ultimately safeguarding both patients and taxpayer dollars.



Data as the Foundation of Integrity and Innovation

Medicare fraud is not just a financial crime—it undermines public trust and diverts resources from patients who need care most. Recent takedowns and government reports demonstrate the sheer scale and global sophistication of these schemes.

The path forward is clear: CMS must adopt a **provider-centric, data-driven model** that replaces siloed systems with a holistic and unified risk view. With LexisNexis Risk Solutions proven capabilities in identity, linkage, and continuous risk monitoring, CMS can stay ahead of bad actors—protecting patients, providers, and the integrity of America's healthcare system.

For more information, please contact us at:
https://risk.lexisnexis.com/government/medicaid-program-management
1-888-216-3544

LexisNexis®
RISK SOLUTIONS

1 https://www.justice.gov/usao-edny/pr/11-defendants-indicted-multi-billion-health-care-fraud-scheme-largest-case-loss-amount
2 https://www.latimes.com/california/story/2022-03-29/fraud-lax-oversight-california-end-of-life-hospice-industry-audit-finds?utm_source=chatgpt.com
3 https://www.gao.gov/assets/gao-23-105494.pdf
4 https://www.gao.gov/assets/gao-24-107487.pdf
5 https://oig.hhs.gov/documents/evaluation/10219/OEI-07-23-00180.pdf

NXR17046-00-1125-EN-US