**Written Testimony of Chris Deery, CFE**
**Director, Corporate Fraud & Investigations, Independence Blue Cross**
**U.S. House Committee on Ways & Means**
**Hearing on Protecting Patients and Taxpayers: Cracking Down on Medicare Fraud**
**April 21st, 2026**

Chairman Smith, Ranking Member Neal, and Members of the Committee—thank you for the opportunity to appear before you today.

My name is Christopher Deery, and I serve as Director of Financial Investigations at Independence Blue Cross, a mission-driven health plan serving nearly three million members, including approximately 175,000 Medicare Advantage and Medicare Supplement beneficiaries in the Philadelphia region.

As a health plan deeply embedded in our community, we see firsthand the impact of health care fraud, particularly when it infiltrates critical benefits like hospice and home health services, which have been identified as high-risk for fraud by federal oversight agencies. Fraud in these spaces diverts resources away from legitimate providers, inflates system-wide costs, and most importantly, exposes vulnerable patients to inappropriate or unnecessary care. It also undermines public trust in programs designed to support our most vulnerable members.

At Independence I lead a multidisciplinary team of investigators, auditors, and data analysts responsible for protecting patients and safeguarding health care dollars across both the Commercial and Medicare markets. Our work focuses on the identification, investigation, prevention, and reporting of fraud, waste, and abuse, and it includes several core functions:

- **Real-time monitoring leveraging machine learning & data analytics**
  We deploy advanced analytics, including machine-learning tools, to assist in analyzing claims activity on a daily basis and monitoring payment dashboards to identify suspicious billing patterns as they emerge. For example, we monitor newly enrolled or out-of-network providers with sudden billing spikes, allowing us to intervene before improper payments escalate.

- **Active investigations to assess payments**
  Our team proactively contacts providers, members, and other stakeholders to validate billed services and confirm clinical appropriateness before improper payments escalate. In addition, we perform field work, when appropriate and consistent with regulatory requirements, to confirm the legitimacy of addresses associated with enrollees and providers.

- **Close collaboration with law enforcement at all levels of government.** We work in ongoing partnership with the U.S. Attorney's Office, State Attorneys General, and local district attorneys to share intelligence, support investigations, and strengthen enforcement efforts. In 2025, our team initiated over 200 investigations resulting in 68 referrals of suspected fraudulent activity to law enforcement partners.

- **Mandatory fraud, waste, and abuse (FWA) training** We require annual FWA training for all employees and key partners to ensure early detection and consistent reporting across the organization.

**Emerging Fraud Schemes in the Medicare Fee-for-Service Program**

Today, our investigations at times uncover coordinated networks involving providers, marketers, and patient recruiters operating through multiple entities to obscure ownership and evade oversight. In many fraud schemes, patients are treated as vehicles for generating improper claims rather than as individuals receiving medically necessary care. Members are often unaware that services are being billed in their names, or that they were never clinically appropriate candidates in the first place. Increasingly, they are targeted through deceptive telemarketing and social media campaigns, which have accelerated with the use of artificial intelligence. Their insurance and medical information have become some of the most valuable data available for sale on the dark web.

The Department of Justice's Operation Gold Rush indictments announced last summer confirmed what many of us in the industry had been sensing: the scale, complexity, and velocity of modern health care fraud far exceed anything seen before. Our health care system has become a routine target for transnational criminal networks seeking large, fast returns.

In the case of Operation Gold Rush, a criminal organization purchased dozens of existing, legitimate medical supply companies to act as fronts to bill Medicare, and Medicare Supplemental Plans, for catheters and glucose monitors that were never provided. The conspirators stole beneficiary information, including Medicare numbers, from elderly or disabled Americans across the country. They were able to launder billions of dollars before being detected.

**These networks are exploiting a simple reality: the structure of the fee-for-service Medicare system makes it inherently vulnerable to fraud.**

While CMS and its contractors do important work, and have made significant strides in recent years, payments in the traditional Medicare program are largely rendered with

limited real-time verification and still resemble a “pay and chase” model that pays claims first and recovers payments later, if ever.

These schemes exploit delays in regulatory review, gaps between Medicare and commercial payer oversight, and the lag inherent in post-payment enforcement. By the time an investigation concludes, significant funds may have been paid, and patients may have experienced months of inappropriate or substandard care.

While payers like Independence Blue Cross have invested heavily in advanced analytics, provider monitoring, and clinical validation, we continue to face structural barriers. The HHS Office of Inspector General and CMS’s Center for Program Integrity have made significant strides, but data sharing remains constrained by regulatory and operational limitations that can slow the timely exchange of actionable information.

**From our experience, meaningful progress in the traditional Medicare program would be supported by three key actions:**

1. **Shifting to proactive monitoring for fraud detection**
   Earlier and smarter intervention, including enhanced pre-payment review and real-time utilization monitoring, is needed, especially in the highest-risk areas such as hospice and home health. Specifically, this would include payments for durable medical equipment and skin substitutes, and whatever the next target becomes.

2. **Better coordination between payers and all levels of government**
   Stronger coordination is needed across CMS, state agencies, private payers, and law enforcement**,** especially in sharing actionable intelligence on emerging schemes and high-risk provider networks once a credible allegation exists. Public-private efforts such as the Healthcare Fraud Prevention Partnership should be strengthened to ensure that actionable information can be shared responsibly as soon as possible. Participation in organizations like the National Health Care Anti-Fraud Association is essential with stakeholders at all levels.

3. **Enhanced oversight of National Provider Identifier (NPIs) systems**
   As learned from Operation Gold Rush and other investigations, fraudsters exploit the NPI system via either outright identity theft of numbers found on the web, obtaining new numbers under false pretenses using fake credentials, or purchasing or transferring numbers from legitimate providers who may be unaware that they will be used for fraud. CMS should systematically flag unusual transfer patterns, changes in ownership, or sudden billing spikes associated with NPIs in coordination with health plans, ACOs, and anti-fraud entities. Provider education also provides an opportunity to mitigate this.

Protecting our members and safeguarding health care dollars—particularly in hospice and home health—is not about limiting access. It is about ensuring program integrity, so these vital services remain available, trusted, and effective for the patients who truly need them. Thank you for your leadership on this issue. I look forward to your questions and our continued collaboration.