The exact amount of money lost each year to healthcare fraud, waste, and abuse (FWA) is difficult to precisely quantify, but estimates typically are in the hundreds of billions of dollars. Although a portion is due to waste, a troubling amount continues to be attributable to fraudulent and abusive practices, ranging from upcoding, overcharging, and medically unnecessary billing to complex collusion.

Here, we describe a fundamental shift in the way in which cases of fraud and abuse are identified and opened. “Turnkey allegations” are created when the burden of vetting and validating fraud allegations prior to opening a case is moved from the health plan’s special investigations unit (SIU) to an unbiased third party.

The process of building a turnkey allegation must be painstakingly thorough and clinically driven, from the development of the analytic models that identify the suspicious claim to the delivery of the case referral to the health plan.
the problem with FWA “business as usual”

Health plan SIUs provide a valuable service in the fight against FWA. Unfortunately, an inordinate amount of plan resources are wasted vetting and investigating leads that often go nowhere.

In fact, Verscend Technologies estimates that SIUs receiving analytics-flagged, unfiltered fraud and abuse allegations—that is, allegations or lead referrals identified through typical claims-based analytic techniques—spend 65 percent of their time, on average, reviewing false positive results. In other words, in an eight-hour day, an investigator spends more than five hours chasing suspicious providers who turn out to be practicing and billing legitimately. That’s not counting the time spent pursuing large numbers of member tips that ultimately turn out to be non-actionable. Investigators become fatigued, and the return does not always surpass the effort.

Gaining access to the data needed to move cases forward—the strong “reason to believe”—is often complicated and time-consuming because the information resides in multiple places within a single organization and/or across multiple organizations. For managed Medicaid plans in particular, which are mandated to report fraud allegations to law enforcement in a timely manner (typically around 10 working days from the time that the alleged fraud is reported to the plan), this data diffusion makes providing the necessary substantiation especially difficult.

In addition, provider relationships suffer when doctors and office staff are asked to respond to SIU inquiries that turn out to be false positives. Providers must often spend precious time providing documentation and may feel wrongly accused and targeted by the health plan.

turnkey allegations defined

Health plans are beginning to deploy their FWA resources more wisely and with greater impact through a new approach called “turnkey allegations.” A turnkey allegation is a ready-to-investigate case referral that has been vetted by an investigative team before the health plan SIU receives it. Instead of simply handing over a list of leads from computer-generated analytics, a team of clinical coding and investigative analysts does the legwork of gathering sufficient evidence to determine which cases are worth pursuing. That intelligence is handed over to the health plan, and an SIU can open the case with confidence.

Typically, a turnkey allegation completes from one-third to one-half of the investigative process before it reaches the SIU, fulfilling the pre-case burden of proof where most of the false positives are identified. As a result, the plan can reduce the time and effort put into pre-case work while increasing its FWA detection success rate.

Building and turning over a turnkey allegation requires:

- **Analytics:** Models must constantly evolve to stay ahead of fraudulent behaviors and recognize patterns of false positives.

- **Clinical, Coding, and Investigative Expertise:** Experts are required to not only design the analytic models, but also thoroughly review leads once they are identified.

- **Technology:** A user-friendly workflow enables analysts to efficiently work a lead while allowing the plan SIU to understand and verify the work that produced the turnkey allegation. Then the SIU can pend any necessary claims for that provider and open the case for further investigation.

not all analytics are created equal

State-of-the-art analytics are the foundation of a turnkey allegation. Analytics must constantly evolve to keep up with changing fraud schemes and shifts in the healthcare industry. Popular fraud schemes used to be very well defined and could be detected with a given set of clinical codes. Today, schemes are increasingly pattern based and may appear legitimate at first glance. Instead of repeatedly abusing certain codes, fraudsters have learned to spread and shift their efforts across multiple schemes.

In addition, changes to the practice environment can erroneously flag claims as fraudulent. For example, 10 years ago, providers sharing a tight network of patients could be seen as collusion. But today, in the world of ACOs, a large number of shared patients may not be suspect.
Analytics that can evolve as healthcare shifts, thus reducing false-positive triggers, have a number of characteristics.

First, they should combine supervised and unsupervised learning. This combination is popular when dealing with large volumes of data and knowledge of the specific type of behavior is limited—in this case, whether or not a provider is fraudulent. This “semi-supervised” approach can build on an existing list of providers to watch and identify providers who share similar characteristics with the fraud cases.

The best analytics also employ ensemble models because, in the world of predictive analytics, the whole is greater than the sum of its parts. Each model has its unique strengths and weaknesses. By combining the models and weighing them accordingly, the weaknesses are mitigated, and models that work better for certain scenarios are more valuable. The ensemble approach of combining strengths and eliminating weaknesses creates a “smart” model that is adaptive.

Ideally, the analytics should also be able to look across multiple, de-identified payer data sets to find abusive or fraudulent providers who otherwise might not draw suspicion based on a single payer’s data. For example, one provider billing eight hours of time to four different payers on the same day would be quickly spotted.

Finally, the analytics should have the ability to run huge volumes of data each day—in the vicinity of billions of claims generated by tens of millions of patients and submitted by millions of providers.

These volumes require vast disk storage and physical memory, as well as tremendous processing capability.

Clinical, coding, and investigative expertise: the human touch

Analytics must be supplemented with human expertise—arguably the most important component of the turnkey allegation. First, the analytic models should be developed and continuously maintained by a well-rounded team of investigators, clinical coders, and data scientists. An interdisciplinary team is critical because each expert has his/her own perspective on what data points are necessary for an investigation, based on each person’s role. Second, once the analytics have identified suspect provider behavior, the pre-case clinical and investigative review begins. The goals at this point are two-fold: eliminate false positives and build a strong reason to believe the allegation.

The investigative analyst team should include people with deep clinical and coding backgrounds in addition to certified healthcare fraud investigators. They must be familiar with the rules of claims coding, be able to match procedures to diagnoses, be adept at reading medical charts, be knowledgeable about common (and in some cases innocent) mistakes, and understand when a physician’s subspecialty does or does not support a certain level of service. They should also easily recognize patterns or connections within the data and make appropriate associations with these patterns and connections when building the allegation.

Finally, as these experts continuously identify true and false positives, this information should be looped back into the models to make them even more effective. Clinical coding experts who are involved in the development of models but not in the operationalization of those models are less effective at ensuring that false positive triggers are reduced.

Technology tools that support decision-making

The analytic technology that supports turnkey allegations should display results in a way that enables users to make quick and accurate decisions. Users will need to drill down into the data for greater detail. Outputs must include the suspect provider and the behavior, of course, but...
also multiple metrics that corroborate the outlying behavior and visualization to help conceptualize the findings. All of this information enables the investigative analysts to hone in on the most promising leads, handing over turnkey allegations in a timely manner.

The technology must also provide allegation summaries with a clear presentation of all facts, a list of the patients associated with the fraud, and recommendations for further action. The patient lists are particularly helpful when the case involves Medicaid fraud, which requires payers to provide a minimum number of patient attestations to support the allegation. This capability saves the plan time hunting down patients to confirm the charge of fraud or abuse.

Finally, technology must be user-friendly, with interactive dashboards, links to claims and other supporting data to save time chasing down information, and functionality that enables cases to be referred directly to state and federal agencies. Additionally, the technology must enable a health plan to immediately suspend future claims payments to a provider while a case is open.

taking unusual drug-screen billing patterns from red flags to turnkey allegation

The red flags: In 2011, a hybrid approach of rule-driven models and data-driven predictive analytics flagged unusual billing patterns for urine drug testing performed at PremierTox, a Kentucky-based toxicology and drug testing lab.

Before handing the lead to the large regional health plan’s SIU, analysts with expertise in medical billing, clinical coding, and investigative research began their work. The analysts were able to access all of the necessary data to review the system-generated red flags, looking at the claim history for PremierTox and drilling down even further into individual patient claim and diagnosis histories.

Using this data, combined with investigative expertise, analysts discovered:

• Billed laboratory services codes for the procedure and diagnosis were nearly identical for each patient visit, as were the number of tests per visit
• The number of tests per visit was very high when compared to other labs, so PremierTox was an outlier compared to its peers
• Many patients were seen and possibly referred by the same doctors
• Many tests had no corresponding office visits

The turnkey allegation: Alone, each activity could have been legitimate. When viewed together by clinical experts, however, suspicious behaviors were validated. With enough evidence in hand, a turnkey allegation was referred to the plan SIU, which opened a case and stopped all further payment of PremierTox claims during the investigation.

The result: The health plan was able to stop payment of all claims pre-pay and did not need to go after any money retroactively. In a settlement before the government got involved, the plan agreed to pay for only the qualitative testing and avoided payment of the more expensive quantitative tests.
the benefits of turnkey allegations

Many health plans estimate that for every 100 to 200 fraud or abuse leads, only one turns out to be actionable. With a turnkey allegation approach, health plans can expect to open 80 to 85 percent of the leads that they receive from their vendor. This novel approach will also:

• Reduce false positives, leaving health plans more time to investigate true cases
• Forestall fraud and abuse earlier, thus preventing future losses
• Make recoveries more likely
• Have a deterrent effect if providers know their claims are being reviewed by outside subject-matter experts

In addition to the financial consequences of healthcare fraud, patients may also suffer serious injury or fatal outcomes at the hands of fraudsters. The quicker fraud can be identified and prosecuted, the sooner these providers are out of business. And when a patient is harmed through fraud, costly and ongoing medical implications can occur that will have to be covered by someone—often the insurer that has already been defrauded.

questions to ask your fraud solution vendor

1. Do clinicians and investigators collaborate with data scientists in the development and maintenance of your analytic models?
2. Do you run your analytics across multiple payer data sets to uncover providers flying under the radar within your own data?
3. What is your average false positive rate?
4. What is your average case open rate?
5. Can I confidently and immediately open a case referred to us by your system?
6. Do your fraud leads come with an expert clinical summary of why they were flagged?
7. Do you provide access to all data sources used in flagging a provider as behaving fraudulently, such as drilling down into full patient histories?
8. Do you identify patients who would have a high likelihood of providing strong evidence for the case?
9. Can I immediately suspend payment of any new claims from within your system for a provider whose case I’ve opened?
10. Can I pull my own provider claims reports from your system?
building better healthcare together

Payment Accuracy
- Claim Accuracy
- Fraud Detection

Revenue Integrity
- Medicare Risk Adjustment
- Commercial Risk Adjustment

Population Health
- Population Health Analytics
- DxCG Intelligence

Quality Improvement
- Quality Reporting
- Record Retrieval
- Record Abstraction

866.292.6971 | info@verscend.com | verscend.com