Medical Waste, Fraud, and Abuse Control

There are some estimates that say as much as $700 billion is lost due to waste, fraud and abuse in the US health care system. (1) That would mean roughly 25 percent of the $2.5 trillion spent on health care, both public and private, in the US is attributable to fraud. Medicaid has been a particularly susceptible target for fraud in recent years, with a distributed management model, limited cross-program communications, and a difficult-to-track patient population of low-income adults, their children, and people with certain disabilities.

Professor Malcolm Sparrow, Harvard University expert on healthcare fraud billing practices and author of the book, "License to Steal," said, " *The government has published annual estimates of improper payment rate for the Medicare program, but the latest estimate says 12.1 percent for Medicare and 9.8 percent for Medicaid. So, we're in the region of 10 percent across both of these programs. And the two of them together have now just gone above $1 trillion this fiscal year. So, if you imagine that the same level of problems are pervasive through these public programs [then] you're looking at a $100 billion,...but I have reason to believe that the estimates that we get from the government are really quite conservative and a little bit comforting because they're based on...methods...[in]sufficient to detect fraud. And everyone associated with those measurement programs knows that. And that has been admitted by government officials in public. So, the real number is higher than 12 percent, but I can't say what it is."*
(2)

There's one thing experts agree on, the amount of healthcare fraud is staggering.

The State of Minnesota spends more than $10 billion a year on health care expenses. If more than 10 percent is fraud, then Minnesota could save nearly $1 billion a year.

Healthcare fraud not only bleeds the system but also represents a colossal injustice as crooks enrich themselves at taxpayers' expense.

Why doesn't our State Colleges and the University of Minnesota teach 'Fraud Control 101?'

Why won't the press address this issue? With the skyrocketing cost of health care, why is fraud neglected by virtually every candidate for public office?

The issue of Waste, Fraud and Abuse in all aspects of government should be a huge issue for candidates for office, for public trust in government, and the efficient use of taxpayers' dollars.

Healthcare fraud has not been brought under control because the government and the health care industry has underestimated the complexity of the fraud-control business and has never developed reasonable defenses against fraud.

The government hasn't found the courage to measure the fraud rate in its major programs. The health care industry provider associations and lobbyists have worked hard to contain and soften the government's fledgling enforcement campaign; they no doubt fear the possibility of a serious and sustained examination of the broader business practices that pervade the industry. But in reality these lobbyists represent an industry-wide business crime wave that day after day swindles hundreds of billions of dollars and, yet, has the nerve to lobby against public enforcement against their crime in the suites.

By learning the art of fraud control the government and the healthcare industry could substantially cut costs without restricting eligibility, denying the needy, or squeezing honest providers out of business.

Addressing Waste, Fraud and Abuse

See "License to Steal-How Fraud Bleeds America's Health Care System" by Malcolm Sparrow

Components of a Model Fraud-Control Strategy

1. Commitment to routine, systematic measurement

2. Resource allocation for controls based upon an assessment of the seriousness (i.e., measurement) of the problem

3. Clear designation of responsibility for fraud control

4. Adoption of a problem-solving approach to fraud control

5. Deliberate focus on early detection of new types of fraud

6. Prepayment, fraud-specific controls

7. Every claim faces some risk of review

8. Detection Systems and Tools

Commitment to routine, systematic measurement

A commitment to routine and systematic measurement is the cornerstone of a fraud-control operation; without it, officials cannot see what they are working on, nor can they tell whether they are making progress. Without measurement, no one can make the case for adequate fraud-control resources.

Healthcare fraud measurement requires:

1. The selection of a statistically valid random sample of claims with

2. A thorough audit of each one; this audit would involve

3. External validation of the information within the claim rigorous enough to identify fraudulent claims.

The sampling should be done soon after the routine operation of control systems. This means that edits and audits and other claim-suspension systems (including medical review) should complete their own review procedures before the random sample is taken. Indeed, fraudulent claims that the system already detects and rejects are not part of the problem to be measured. The important measure is the volume of fraudulent claims paid – which represents the proportion of program costs lost to fraud. Only by allowing detection systems to operate first, before taking the sample, can one determine what those systems miss. Just as it would be a mistake to take the samples too early, it would also be a mistake to take them too late. *The goal is not to prove criminal intent beyond a reasonable doubt, but to see how bad things are and to determine whether they are getting better or worse.*

Judgments auditors and investigators can make in a rigorous claims review are:

· Does the service or product appear to have been supplied as claimed?

· Did the patient suffer from the condition corresponding to the diagnosis entered on the claim form?

· Can the referring physician confirm his or her referral?

· Would the claim, if all these surrounding facts had been known when the claim was

processed, have been paid?

Political problems are harder to overcome than the technical problems because managers will remain nervous about the prospects of having to reveal the results of such measurements. Some fear that even if they discover the true extent of fraud, they would be unable to bring it under control. Some prefer not to know. Some try to preserve their own interests, will do whatever they can to sabotage measurement studies that might reveal bad news. As painful and difficult as it may be, a model fraud-control strategy requires a commitment to systematic measurement.

Resource Allocation for Controls Based Upon the Seriousness of the Problem

Under a model fraud-control strategy, investment in control systems (people and technology) would be related in some direct and obvious way to the size of the problem as determined by measurement. Budget increases for fraud control have been restricted in the past due to a lack of measurement even though more fraud control resources were better than less.

Clear Designation of Responsibility for Fraud Control

In most organizations, nobody has full responsibility for fraud control, allowing the fraud perpetrator to design scams that chart a course around each isolated function until nobody is left to oppose them.

A fraud control executive, or fraud control unit, whose job is to focus on fraud rather than other internal functions must be given overall responsibility for all aspects of fraud control, with the freedom to design new policies and procedures, to target investigations and examinations of particular aspects of the problem, and to propose changes in regulation.

A common mistake is to equate fraud investigation with fraud control. Investigation is a valuable tool in the control toolbox, but it’s not the whole toolbox. The performance of a fraud-control unit should be measured by its success in lowering or suppressing the level of fraudulent claims the system pays, which would be measured periodically. Target levels would

be set; these could be lowered year after year as the control operation matured until the fraud level was low enough to be regarded as “an acceptable price of doing business.”

A Problem-Solving Approach to Fraud Control

Enforcement officers point out, correctly, that no preventive operation can be successful enough to make a reactive capacity unnecessary. Investing everything in prevention is as foolish as investing everything in enforcement. Unfortunately, bitter and destructive internal battles divide people into camps.

Switching to a *Problem-Solving or Compliance Management* approach rescues regulatory agencies from these destructive tensions and provides a constructive way forward.

A problem-solving strategy picks the most important tasks and then selects appropriate tools in each case; it does not decide first which are the important tools and then pick tasks to fit. A problem-solving operation organizes the tools around the work, not the work around the tools, changing the unit of work from cases to problems.

Stages of Problem Solving

Stage 1: Nominate Potential Problem for Attention

Stage 2: Define the Problem Precisely

Stage 3: Determine How to Measure Impact

Stage 4: Develop Solutions/Interventions

Stage 5(a): Implement the Plan

Stage 5(b): Periodic Monitoring/Review/Adjustment

Stage6: Project Closure, and Long-Term Monitoring/Maintenance

At a minimum, successful adoption of the Herman Goldstein problem-solving approach to fraud control will combine the following features:

· A deliberate and continuing commitment to search for new and emerging patterns of fraud.

· A person or team of people clearly designated as responsible for fraud control, with access to and influence over the whole range of functional tools—from the design of eligibility criteria at one end of the process, to investigation and prosecution at the other end.

· Conscious recognition of the fraud *problem* as the relevant unit of work, producing a project focus rather than a case-by-case focus.

· A focus on effectiveness (as opposed to outputs), with a commitment to monitoring the impact for each problem tackled.

Deliberate Focus on Early Detection

A model fraud-control strategy must stress early detection of emerging fraud problems rather than remaining in a reactive posture and waiting until the problems, much enlarged, threaten to

overwhelm.

Resources must be set aside for proactive outreach and intelligence-gathering operations, and these resources must be protected from the demands of the reactive workload—otherwise proactive activities will never survive.

Here are some proactive tools:

· Establishing and maintaining a network of contacts with other insurers and law-enforcement agencies to provide early warning of fraud trends already spotted by others;

· Conducting undercover operations, such as “undercover shopping” of newly established storefront clinics (the object being to find out what kinds of services are really being provided, and to whom);

· Developing informants who can report on emerging practices within criminal networks;

· Interviewing convicted fraud perpetrators who may be willing to describe a variety of fraud methods and whom may be able to point out vulnerabilities in payment systems;

· Data mining: using a broad range of analytical tools to search for anomalous patterns

· Employing focus groups to pick the brains of patients and providers about system vulnerabilities and observed patterns of suspicious behavior;

· Educating claims processing staff (those few who retain the opportunity to examine the contents of claims) about indicators of fraud; and

· Creating “tiger teams” within the organization (whose job is to come up with creative new ways to cheat the system) as a way of testing and refining defenses.

A collection of such activities constitutes an intelligence operation that may generate cases, but not case-based. The objective is to discover emerging fraudulent practices so that the control operation can find antidotes.

Fraud-Specific Prepayment Controls

The fraud-control team must be able to operate prepayment as well as post-payment; this means they should be able to insert their own fraud-specific edits and audits into the processing system. The team should have their own resources to validate suspended claims instead of relying on medical review teams (already overburdened and focused on different issues) to do it for them; and they have to be able to design and operate their own focused reviews, randomly selecting claims within fraud-prone areas and using external validation procedures—telephone calls, visits, on-site audits—to check them out.

The fraud-control team must be able to prevent rapid, high-dollar-value fraud schemes, characterized as bust-outs; they must have the capacity to operate the types of controls (which are invariably missing) that eliminate this threat. These controls would involve, at a minimum, automatic suspension of high-dollar payments (above some arbitrary threshold) pending human review of the contributing claims; provider-level monitoring (looking for sudden accelerations in aggregate claims levels, or totals in excess of reasonable norms for that specialty); and the routine random selection of a small portion of claims for validation.

Whoever is given responsibility for fraud control needs the freedom to intercept claims prepayment rather than operating entirely post-payment.

Every Claim Faces Risk of Review

Every claim submitted for payment should suffer some risk of review for fraud, no matter what its dollar value, regardless of its medical orthodoxy, and regardless of the reputation of the claimant. When reviewing claims before payment, the fraud-control team should be responsible for extracting claims for random review and making inquiries to establish the legitimacy of each one. Such a provision would go a long way toward eliminating the vulnerability of payment systems to massive computerized billing schemes—one of the most worrying modern threats. When prepayment inquiries show a claim to be even a little suspicious, and do it reasonably quickly, the fraud-control team can then suspend all claims pending from the same source and subject them to detailed scrutiny.

The industry will raise two objections to such a practice. First, they will say that random selection, with external validation, constitutes an arbitrary and unwarranted intrusion into the affairs of perfectly respectable providers, however, such an intrusion may be part of the price society has to pay for reasonable protection of the health care system. Government and insurers cannot control costs if they give up the right to verify the truthfulness of claims.

Second, industry officials will point out that scarce audit and investigative resources would be better used on focused claims review than on random review. But focused reviews serve a different purpose and cannot offer the same protection that random reviews provide because fraud perpetrators watch to see where insurers are focusing and then deliberately play elsewhere.

The probability of review should *never* be zero—not for any provider, no matter how reputable; not for any claim, no matter how small.

Detection Systems and Tools

The Seven Levels of Health Care Fraud Control

Level 1: Claim, or Transaction Level

Level 2: Patient/Provider Relationship

Level 3: (a) Patient Level

(b) Provider Level

Level 4: (a) Patient Group/Provider

(b) Patient/Practice (clinic)

Level 5: Policy/Practice Relationship

Level 6: (a) Define Groups of Patients (e.g., Families or Residents of One Nursing Home)

(b) Practice (or Clinic)

Level 7: Multiparty, Criminal Conspiracies

The current emphasis of fraud detection tools fall within certain narrow categories.

Prepayment Monitoring– Edits and audits within claims-processing systems perform monitoring at the transaction level (Level 1) and at the patient level (Level 3 [a]). Transaction-level picks out claims where the diagnosis doesn't match the procedure code; where the age or gender of the patient does not match the diagnosis; or where detectable forms of unbundling or price manipulation have occurred. Patient-level monitoring examines each claim in the context of the patient's recent claims history like frequency of certain procedures, incompatible treatments, etc.

Post-payment Monitoring– The vast majority falls at Level 3 (b), taking the form of provider profiling. Profiling systems calculate a set of variables or ratios for each provider descriptive of their overall treatment patterns that appear anomalous against the background of their peer group.

The industry's detection toolkit is focused on levels 1 and 3; prepayment monitoring and post-payment monitoring.

Ideally, payment systems should be protected at all levels and at the earliest moment. Unfortunately, the industry falls into the trap of using technology to enhance *existing* detection capabilities rather than to build new capabilities.

It is much easier to throw fashionable new technologies (such as neural networks, artificial intelligence, or advanced statistical methods) at traditional forms of analysis than to understand the need for new forms of analysis. The use of more sophisticated tools ends up displacing human judgment and expertise rather than equipping it.

Instead of focusing upon state-of-the-art analytical methods, the industry should focus on providing its fraud-control teams a range of flexible, user-friendly claims analysis tools. These teams should be able to construct their own searches quickly and easily, slicing and dicing the claims data in many different ways, inserting and deleting different types of search as different fraud threats wax and wane. The most important tools in the fraud-detection toolkit are timely and easy access to claims data (including prepayment data); friendly, easy-to-use non-technical interfaces; and a broad range of analytical tools that can be easily sequenced to answer complex ad-hoc inquiries.

Defense at the Higher Levels

One major opportunity to apply modern technology to great effect for fraud control lies in the development of detection tools aimed at the highest levels (Levels 6 and 7). The healthcare industry currently has almost no capacity to monitor at such levels, and it certainly has no warning systems that can detect the most sophisticated schemes early enough to prevent major

losses. These schemes, involving extensive collusion, operate across multiple patients, multiple providers, and often across multiple insurers. These schemes are designed and operated to be undetectable by lower-level detection tools.

For many institutions facing fraud committed by organized criminal rings, transaction-level and other lower-level defenses are no longer enough. As the perpetrators shift their attention to multi-account schemes, so the defending institutions have to develop multi-account or ring-level detection systems that can spot major schemes early enough to cut them off and make them unprofitable.

(1) Where Can $700 Billion In Waste Be Cut Annually From The U.S. Healthcare System? http://blr.healthleadersmedia.com/content/241965.pdf

(2) 06-25-2016 Ralph Nader Radio Hour http://ralphnaderradiohour.libsyn.com/michael-shuman-malcolm-sparrow

Predicting Healthcare Fraud in Medicaid: A Multidimensional

Data Model and Analysis Techniques for Fraud Detection (2013)

http://doc.utwente.nl/96578/1/1-s2.0-S2212017313002946-main.pdf

Using Data Mining to Detect Health Care Fraud and Abuse: A Review of Literature

http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4796421/

Improving Fraud and Abuse Detection in General Physician Claims: A Data Mining Study

http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4770922/#s4title

Computer-aided auditing of prescription drug claims.

http://www.ncbi.nlm.nih.gov/pubmed/23821344

{jsmallfib [top]}