U.S. Department of Justice
Office of Justice Programps
National Institute of Justice

National Institute of Justice

Research in Brief

Jeremy Travis, Director

December 1998

Fraud Control in the Health Care Industry: Assessing the State of the Art

by Malcolm K. Sparrow

Issues and Findings

Discussed in this Brief: The health care industry's traditional approach to fraud control, the weaknesses of that approach, and the essential elements of more effective fraud control systems.

Key issues: The incidence of health care fraud remains at alarmingly high levels despite unprecedented attention in recent years from policymakers and law enforcement. Major scams appear to be artfully designed to circumvent routine controls and may remain invisible for long periods. When they are discovered, it seems often to be more by luck than judgment.

Key findings:

- Fraud control is more complex and difficult than is usually appreciated. Officials responsible for payment safeguards generally receive no formal training in fraud control.

- Certain factors make fraud control particularly difficult in the health care industry, including the social acceptability of government and insurance companies as targets for fraud, and the degree of trust society places in health care providers.

- Most insurers, public and private, have failed to measure systematically the fraud problem they face. Oblivious to the

continued…

More than $1 trillion is spent on health care each year in the United States, roughly 15 percent of the gross national product. The proportion of annual health care expenditures lost to fraud and abuse remains unknown because such losses are not systematically measured. But conventional wisdom, supported by recent Medicare studies undertaken by the Office of Inspector General, U.S. Department of Health and Human Services,[1] estimates that losses to fraud and abuse may exceed 10 percent of annual health care spending, or $100 billion per year.

Since 1992, when health care reform emerged as a matter of national debate, the issue of fraud control has received much attention. For example, health care fraud remains a top priority of the U.S. Department of Justice, with criminal convictions in 1997 increasing threefold over the 1992 total;[2] and over the past several years, the Federal Bureau of Investigation (FBI) has markedly increased the number of agents assigned to its health care fraud unit.

Such unprecedented attention to the issue of health care fraud produced many apparent successes. Coordinated actions involving Federal and State authorities as well as private insurers have succeeded in identifying health care fraud and abuse committed by major corporations. Nonetheless, little progress—in terms of practical improvements—seems to result. Not one of the industry officials interviewed in connection with this research thought the situation was under control or even in the process of being fixed. The majority thought existing efforts to control the

Related reading

A slightly more technical presentation of some of the material in this Research in Brief is found in the article "Health Care Fraud Control: Understanding the Challenge," published in the *Journal of Insurance Medicine*, 28 (November 1996):2, 86–96. We are grateful to the publication's managing editor, Dr. Nigel Roberts, for his permission to use information from the article in this Research in Brief.

A complete account of Dr. Sparrow's research and findings on health care fraud may be found in his book *License to Steal: Why Fraud Plagues America's Health Care System*, Denver: Westview Press, 1996. Available from Westview: 303–444–3541.

Issues and Findings

continued…

magnitude of the problem, they massively underinvest in fraud control.

- Existing fraud control arrangements, such as claims processing "edits and audits" and utilization review, appear very useful in correcting honest billing errors and in detecting unorthodox medical practice, but ineffective in detecting criminal fraud. Fraud perpetrators can easily circumvent such controls by billing "correctly" and staying within the confines of medical orthodoxy and policy coverage, even as they lie. The rule for scam artists becomes "bill your lies correctly."

- The ubiquitous advent of highly automated claims processing mechanisms, with electronic submission and electronic payment, presents new dangers for fraud control. Some believe that comprehensive batteries of up-front edits are sufficient to defend such systems. But such belief ignores the dynamic nature of the fraud game, underestimates the abilities of fraud perpetrators to test the system, and overlooks the critical role that human beings must play in effective fraud control.

- Under capitated managed care programs, the principal forms of fraud involve diversion of capitation payments away from frontline service delivery, resulting in patterns of underutilization that may be more dangerous to human health than traditional fee-for-service fraud schemes.

Target audience: State and local legislators and policymakers, law enforcement agencies, prosecutors, health care administrators and insurers, and researchers.

problem barely scratched the surface, and how much fraud one found in the system depended only on how hard one looked:

- In 1994, the administrator of the Health Care Financing Administration (HCFA) acknowledged "good reason to believe" that the $5.4 billion in recoveries involving Federal health programs during that year was "merely the tip of the iceberg."[3]
- In March 1995, the FBI's director stated that intelligence showed cocaine traffickers in Florida and California were switching from drug dealing to health care fraud (the latter being safer, more lucrative, and less likely to be detected).[4]
- In early 1998, a scheme surfaced whereby more than $1 billion in phony medical bills using the names of unsuspecting patients and doctors had been submitted to scores of private insurers nationwide.[5]
- In July 1998, a Medicare contractor agreed to pay $144 million in civil and criminal penalties for concealing evidence of its poor performance in reviewing and paying claims of Medicare beneficiaries,[6] and receiving $1.3 million in Government performance bonuses to which it was not entitled.

Many instances of health care fraud suggest that existing control systems do not work the way we imagine they should. Often the manner in which schemes are revealed suggests detection is more luck than system. General Accounting Office (GAO) testimony to Congress has cataloged instances of fraud in the Medicare and Medicaid programs that, according to GAO, ought clearly to have been detected and stopped.[7] But in each case the schemes came to light only through tipoffs or whistleblowers, rather than through the operation of routine monitoring or audit.

In one case, a pharmacist from California had been billing Medicaid for improbably high volumes of prescription drugs and was being reimbursed without question, despite several recipients receiving more than 20 prescriptions per day.[8] For another patient, Medicaid paid for more than 142 lab tests and 85 prescriptions in 18 days.[9] All these transactions turned out to be fraudulent, yet none was picked up by routine monitoring or detection efforts.

In short, despite the level of political, legislative, and administrative attention paid to the fraud issue in the last several years, disturbing and somewhat surprising lapses in control persist.

The study summarized by this Research in Brief examined the health care industry's fraud control apparatus and asked, "Does it work?" and, if not, "Why not?" (See "Study Methodology.") It assessed the assumptions, policies, and machinery comprising the health care industry's approach to fraud control in an effort to understand strengths and weaknesses and to offer some clues about how to make controls more effective.

Focus on criminal fraud

This study focused quite deliberately on criminal fraud as opposed to abuse, despite the difficulty of drawing a clear line between them. The reason for focusing on fraud rather than abuse (or billing errors, or "code optimization," or a host of other gray areas) is that fraud controls play to a distinctively different audience. Control systems may work very well in pointing out billing errors to well-intentioned physicians and may even automatically correct errors, adjust claims, and limit manipulation of billing codes. But those same systems may offer no defense against determined, sophisticated thieves, who treat the need to bill "correctly" as the most minor of inconveniences.

Study methodology

Background knowledge of the health care fraud issue was derived from literature searches and from 4 years (1992–96) of interaction with concerned public and private organizations, including the U.S. Department of Justice; Federal Bureau of Investigation; Health Care Financing Administration, Office of Inspector General (U.S. Department of Health and Human Services); Health Insurance Association of America; National Health Care Anti-Fraud Association; and the National Association of Medicaid Fraud Control Units.

Eight sites for field work were selected in consultation with an advisory committee, including representatives from the above organizations and the National Institute of Justice, which funded the study.

All eight field sites were selected in part because they were reputed to be among the best in the industry in terms of fraud control. The reason for selecting from among the best, rather than picking a broader or more representative sample, was to work from current best practice, so that any guidance ultimately offered to the industry would help advance the state of the art.

The sites were also selected to offer, as far as possible with only eight, a broad cross section of the industry. The sites examined included three Medicaid Fraud Control Units, two private insurers (one large, one much smaller), and three private corporations acting as Medicare contractors, all three of which were among the top five Medicare contractors in terms of total claims volume. One of these contractors also served as a durable medical equipment regional contractor (DMERC). As one of four designated DMERC sites, this company processes durable medical equipment claims under the Medicare program for roughly one-quarter of the United States.

The eight sites selected agreed to participate in the study and to make managers and staff available for interviews. A list of 15 interview subject areas was provided in advance to each site, with a request that interview lists be constructed to include personnel knowledgeable in each area. Beyond that, the interviews themselves were not formally structured.

Most competent fraud perpetrators study the rule book carefully—probably more carefully than most honest providers—because they want to avoid scrutiny at any cost. So they "test" claims carefully, making sure they neatly pass all the established system edits and audits. Then, having found combinations of diagnoses, procedures, and pricing that "work" (i.e., trip no alarms and preferably pass through "auto-adjudication" to payment, avoiding human scrutiny altogether), they ratchet up the volume, carefully spreading the claims activity across different patients and across different insurers to avoid detection.

Many control systems are designed with only one audience in mind—honest providers, perhaps error prone, perhaps not up to date on administrative requirements and regulations, on occasions sloppy and disorganized, often confused by complex or indecipherable rules. For this audience, control systems serve the purpose of correcting errors, testing eligibility, matching diagnoses to procedure codes, checking pricing, and, if necessary, sending claims back for correction.

But effective fraud control systems must deal with quite a different audience: sophisticated, well-educated criminals, some medically qualified, some technologically sophisticated, all determined to steal as much and as fast as possible. They read manuals, attend seminars, and really appreciate all the help and training they can get in how to bill correctly, how to avoid prepayment medical review, and how not to "stick out" under postpayment utilization review.

That second audience is the one that counts here. The study evaluated fraud control assumptions, policies, and systems in terms of their effectiveness in deterring, preventing, and detecting *criminal fraud*.

What makes fraud control difficult and complex?

Fraud control—in *any* profession—is a miserable business. Failure to detect fraud is bad news, and finding fraud is bad news, too. Senior managers seldom want to hear news about fraud, because such news is never good. Institutional denial of the scope and seriousness of fraud losses is the norm. Fraud control policies tend to be shortsighted and scandal driven.

The following seven factors largely explain what makes fraud control, in any environment, such a difficult and complex challenge.

1. What you see (i.e., what your detection systems show you) is never the problem. Most white-collar frauds fall in the category of "non-self-revealing" offenses. Unless they are detected close to the time of commission, they will likely remain invisible forever. Thus you see only what you detect. The danger, of course, is that organizations vulnerable to fraud lull themselves into a false sense of security by imagining that their "caseload" (i.e., what they detect) reflects the scope and nature of fraud being perpetrated against them. Often it represents only a tiny fraction, and a biased sample, of the frauds being perpetrated.[10]

2. Available performance indicators are at best ambiguous; at worst, perverse and misleading. If the amount of detected fraud increases, that can mean either the detection apparatus improved or the underlying incidence of fraud increased. The resulting ambiguity pervades much fraud control reporting.[11] Many other quantitative measures of fraud control success are ambiguous too. Successes in detection and prosecution can equally be viewed as failures in prevention. Some organizations boast of "record recoveries"; others say they prefer to deter fraud up front and regard chasing monetary recovery after the fact as a poor second best. Some organizations emphasize prevention to avoid having to admit that their detection systems are ineffective.

3. Fraud control flies in the face of productivity and service and competes with them for resources. A layer of fraud controls tends to slow down or complicate routine claims processes and creates too many categories for exceptional treatment. Officials responsible for high-volume claims processes want to think about the best way to handle the whole load. Investigators or fraud analysts want to think about the best way to handle the exceptions.

The savings from processing efficiencies may be small, but they are concrete and tangible. By comparison, the potential savings from enhanced fraud controls may be massive, but they remain uncertain and invisible. Bureaucracies usually choose concrete and immediate monetary returns instead of longer term, uncertain ones. So processing efficiency usually wins the battle for resources. As a senior HCFA official pointed out to the author, "Of course, the cheapest way to process a claim is to pay it."

4. Fraud control is a dynamic game (like chess), not a static one. Fraud control is played against opponents who think creatively, adapt continuously, and relish devising complex strategies. So a set of fraud controls that is perfectly satisfactory today may be of no use tomorrow, once the game has progressed a little. Maintaining effective fraud controls demands continuous assessment of emerging fraud trends and constant, rapid revision of controls.

5. Too much reliance is placed on traditional enforcement approaches. The strength of the deterrent effect depends on the probability of getting caught, the probability of being convicted once caught, and the severity of the punishment once convicted. For white-collar crimes all three of these are notoriously low; hence effective investigations do not necessarily translate into effective control. Many organizations fail to make the distinction between investigation (a tool) and control (the goal). Investigation focuses on detected cases, whereas the control function seeks to uncover and grapple with the invisible mass.

6. The effectiveness of new fraud controls is routinely overestimated. A false optimism is based on the hope that elimination of the types of scams most recently seen will mean elimination of the fraud problem. This fails to take into account the adaptability of opponents, who take only a few days, or weeks at most, to change tactics once they find a particular method thwarted.

7. Fraud control arrangements reflect the production environment within which they operate and thus address only the least sophisticated fraud schemes. Fraud controls are typically superimposed upon or embedded within high-volume, repetitive, transaction-oriented processes. Consequently fraud controls, consisting of a set of filters or branch points embedded within the transaction-processing operation, examine claims or transactions one at a time and usually in the same order in which they arrive.

This approach faces two major problems. First, the fraud control game is dynamic, so a static set of filters has only short-term utility. Second, most sophisticated fraud schemes are devised by perpetrators who assume the existence of transaction-level filters and who therefore design their fraud schemes so that each transaction comfortably fits a legitimate profile and passes through unchallenged. Fraud controls of this obvious "transaction level" type generally detect only the casual, careless, and opportunistic fraud attempts, not those of the serious dedicated criminal groups who quickly progress to a higher level of sophistication.

Exacerbating factors in health care insurance industry

The factors above suggest that fraud control is a more complex and difficult challenge than is usually appreciated. Within the health care industry, additional factors exacerbate the problem.

Insurers seen by significant segments of the population as socially acceptable targets for fraud. Insurers are seen as "large, rich, anonymous, and as fair game for fraud in much the same way as tax authorities."[12] Health care fraud causes financial losses primarily to insurance companies and government bureaucracies, targets that engender little public sympathy.

Majority of health care fraud schemes "non-self-revealing." Many interviewees shared the common public assumption that explanations of medical benefits (EOMBs) sent to patients provide protection against provider fraud. But EOMBs do not have the effect one would hope, for a number of reasons:

- EOMBs are not sent to patients in many circumstances. Use of EOMBs is no longer routine within the Medicaid program. Under Medicare, EOMBs traditionally are mailed only when services require a copayment or Medicare refuses to cover a service. So, when services are approved and reimbursed 100 percent by the program, EOMBs normally have not been sent—in which case Medicare beneficiaries have no way of knowing what was billed under their names. Since 1981, EOMBs have not been used in connection with home health care services, now one of the most fraud-prone areas.
- Recipients of EOMBs have little or no financial incentive to pay attention to them. They are not, as in the case of a credit card statement, being asked to pay a bill.
- Many recipients cannot decipher the strange, computer-generated forms and have no incentive to try.
- Fraudulent suppliers find innovative ways to stop patients from reading their EOMBs, such as offering to buy back unopened EOMB envelopes or changing patient addresses on claim forms, thus diverting EOMBs to mailboxes under the suppliers' control.
- Many fraud schemes deliberately target vulnerable populations, such as the elderly or Alzheimer's patients, who are less willing or able to complain or alert law enforcement.[13]
- Even when beneficiaries call insurers to complain about bogus or questionable charges, the handling of beneficiary complaints often lacks the rigor required to uncover fraud.[14] The non-self-revealing nature of nearly all health care fraud schemes decreases the likelihood that authorities will be aware of the true scope and nature of the fraud problem.

Separation between administrative budgets and "funds." Investment in adequate fraud controls suffers significantly because program administration costs are budgeted separately from program costs (i.e., claims paid). This budgetary separation makes it virtually impossible to consider the notion of "return on investment" in allocating resources for fraud control.

The separation is most stark under Medicare Part A. The Medicare trust fund for Medicare payments under Part A is maintained by the 3.3 percent Medicare payroll tax, paid equally by employers and employees.[15] Medicare's administrative expenses, by contrast, come out of a "discretionary budget" from general tax revenues. In 1995 GAO observed that payment safeguards under the Medicare program produced at least $11 for every $1 spent; yet, on a per-claim basis, Federal funding for safeguard activities declined by more than 32 percent since 1989; adjusted for inflation, it fell 43 percent.[16]

In other governmental and nongovernmental programs, the separation, whether statutory or merely administrative, is powerfully manifested in employee culture and attitudes. Most officials care a great deal either about the costs per claim (where their goals and incentives all relate to efficiency) or about payment accuracy. Which one they care about depends on their specific responsibilities. Few managers find themselves in a position to understand the essential balance between them.

Respectability of the health care profession. The degree of trust society places (quite appropriately) in its health care professionals makes effective fraud control yet more difficult. Revelations about fraud are received by medical practitioners as an attack on the integrity of the profession and on its ability to police itself. Thus, the profession and its associations tend to play down the extent and seriousness of health care fraud and to oppose additional resources for investigation and review.

The respectability of the medical profession also presents notable problems to investigators and prosecutors. Investigators, lacking medical training, feel sorely disadvantaged when questioning physicians, whom they frequently experience as arrogant and condescending. And most prosecutors still avoid taking cases that require expert medical testimony, knowing they will be difficult, expensive, and relatively unlikely to succeed in front of a jury. Some prosecutors still display a broader reluctance to bring physicians—pillars of the community—to trial.

Perhaps most damaging, health care insurers extend the same kind of professional immunity and trust to all kinds of other provider groups whose members are not bound by a formal code of professional ethics—durable medical equipment suppliers, home health care agencies, medical transportation companies, physiological laboratories, etc. Payers accord such groups surprising latitude, paying claims on trust without any routine external verification of services provided.

Absence of clear distinctions between criminal fraud and other forms of abuse. Criminal fraud is clearly enough defined, requiring a deliberate misrepresentation or deception leading to some kind of improper pecuniary advantage. But when the deception or misrepresentation relates to the question of medical necessity, the distinctions between fraud and abuse become quite muddy.

Definitional ambiguities between criminal fraud and other forms of abuse produce some troublesome consequences for fraud control. First, they contribute to the medical profession's reluctance to unequivocally condemn fraudulent practice. (Nobody could be sure where along the continuum that condemnation, once mobilized, would end. Physicians may find it hard to condemn fraudulent practice among their peers if they cannot draw satisfactory dividing lines between what they might condemn in others and what they do themselves.)

Second, definitional ambiguities make it much more difficult to measure the problem systematically, because any measurement methodology would have to establish clear outcome classifications.

Third, definitional ambiguities provide an excuse for anyone who would prefer, for whatever reason, not to refer suspected "fraud" cases to an investigative unit. Many payment agencies, protective of their provider network and their program's public image, prefer to handle even quite serious cases through administrative action rather than turn them over to an investigative unit.

These impediments to effective fraud control—social acceptability of government and insurers as targets of fraud, invisible nature of the crime, separation of administrative budgets from "funds," trust placed in providers, and difficulties of separating fraud from other forms of abuse—are substantial. Add to them the seven elements noted previously under "What makes fraud control difficult and complex?" and the task of controlling fraud seems particularly complex, amorphous, and overwhelming.

Perhaps this helps begin to explain why health care fraud has not gone away despite the attention paid to it and why strenuous political and administrative efforts to bolster defenses have failed to provide a convincing cure. Another reason, which this study has established, is that the policies, systems, and machinery currently in place to combat fraud cannot possibly provide effective control. They are no match for the task.

Absence of measurement

The health care industry differs from some other fraud control environments in its ubiquitous failure to measure the problem. The failure to systematically and routinely measure the scope of fraud is characteristic of the whole insurance industry—not just health care—and is not limited to the United States.[17] Measurement of fraud losses is quite feasible; it would involve standard sampling techniques backed by rigorous claims audits involving external validation procedures sufficient to identify fraud if present.[18] Success with such techniques has been demonstrated by the Internal Revenue Service in its efforts to measure and control fraudulent claims for tax refunds based on the earned income tax credit.[19]

Many interviewees believed that their companies' quality control procedures served the measurement function. However, without exception, such programs measured procedural compliance, accepting the claim as presented, and made no attempt to check the veracity of the information in the claim itself.[20] As Clarke's 1990 study of insurance fraud pointed out, "the essence" of any fraudulent insurance claim "is to appear normal and to be processed and paid in a routine manner."[21] One of the surprising truths of the fraud control business is that fraud works best when claims processing works perfectly.

Resource allocation in the absence of measurement

In the absence of scientific measurement of health care fraud, the debate focuses on the size of the problem rather than on the search for solutions. Consequently, massive underinvestment in fraud control resources seems to be the industry norm.

Spending on payment-safeguard activities within the Medicare program totaled $441 million in fiscal year 1996. With a total Medicare budget of approximately $160 billion,[22] this represents an investment in fraud control of less than 0.3 percent of overall program costs—to tackle a problem whose size is estimated at more than 10 percent of program costs. These investments, small as they are, pay off handsomely. The special investigative units at Medicare contractors all save more than they cost, several producing savings-to-costs ratios as high as 14:1.

In the Medicaid program, total spending on the Medicaid fraud control units runs at roughly 0.05 percent of total program budget. The Federal Government offers to pay $3 for every $1 the States invest in their fraud control units, with a cap for Federal reimbursement at 0.25 percent of the State's annual Medicaid budget. Despite the $3-for-$1 offer, most States have for many years chosen to operate at a funding level far below the reimbursement cap.

A clear pattern emerges, spanning both commercial and public health insurance programs. The extent of fraud is never measured, merely estimated. The estimates are too soft to act as a basis for serious resource allocation decisions, so resources devoted to fraud control have to be based on something other than the perceived size of the problem. In practice, control resources are budgeted incrementally, with significant increases likely only if a fraud unit is visibly drowning under its caseload.

In practice, most fraud units, however small, are not drowning. The most likely explanation—which the field work for this study revealed all too clearly—is that the referral mechanisms do not work very well, producing the merest trickle of cases compared to the underlying size of the problem.

Assessment of existing fraud control apparatus

A central focus of this study's field work was to examine the units, functions, and systems that constitute existing fraud control arrangements: claims processing "edits" and "audits," claims development, prepayment medical review, postpayment utilization review, and special investigative units. These controls appear to be extremely useful for correcting providers' honest errors but ineffective as detection apparatus for criminal fraud. Fraud perpetrators can easily circumvent such controls by billing "correctly" and staying within the confines of medical orthodoxy and policy coverage.[23]

Claims processing edits and audits. These edits and audits enable the system to pay the right amount to the right person for the service claimed. They serve to correct billing errors and inappropriate billing procedures. And they reject claims if one or more of the provider, recipient, or procedure is somehow ineligible. But such systems do nothing to verify that the service was provided as claimed, or that the diagnosis is genuine, or that the patient knows about the alleged treatment. Rather, they assume the information presented is true and consider whether that information justifies payment of the claim.

Of the industry's standard edit and audit software modules, none is targeted on fraud. Generally, no attempt is made to create rules or logic to pick out "suspicious" claims for closer scrutiny or to detect claims containing deception or misrepresentation. The industry does not use fraud-specific prepayment edits or audits of any kind.

Claims examination. Once humans have a chance to inspect claims, the prospects for fraud detection and referral improve tremendously. Humans, given the opportunity, often notice the unusual or incongruous. The usefulness of this detection opportunity is constrained, however, because claims are suspended for review only if they trip a condition specified by the system audits. The model is "Systems Select: Humans Inspect." And the basis upon which claims are selected for review seldom has to do with fraud.

Prepayment medical review. This function's purpose is to establish medical orthodoxy and necessity and to determine whether the treatment is reimbursable. Often medical reviewers do spot fraud, but that is a fortuitous by-product of the fact that they are human and are looking at the claim, not because it is their job. Medical review and fraud detection are quite separate sciences. To escape attention from medical review, fraud perpetrators have only to base their false claims on medically plausible diagnoses and procedures and to stay comfortably within the confines of policy coverage.

Postpayment utilization review. Utilization review is currently the major tool used by the industry to detect fraudulent patterns of claims, with "provider profiling" being the predominant form of analysis. The degree to which postutilization review turns out to be a useful device for fraud control depends upon the degree to which fraud perpetrators use anomalous billing patterns. Of course, the smart ones do not.

Once again, this is not a criticism of postutilization review procedures per se. The principal purpose of utilization review is to review medical utilization patterns, both on an aggregate basis (to help formulate policy changes or provide needed provider and recipient education) and on an individual-provider basis (to eliminate medically inappropriate or unreasonably expensive treatment). As a fraud detection methodology, however, postutilization review procedures, with their strong emphasis on provider profiling, have certain limitations:

- They detect fraud only where it produces anomalous billing patterns. This makes them much better suited to detecting waste and abuse that does not amount to criminal fraud.
- Utilization review generally leads to scrutiny of only a few extreme outliers within each provider category, leaving the bulk quite safe from detection, even if the bulk is rotten.
- Most utilization review units prefer to inform and educate providers when they detect anomalous billing patterns, rather than investigate. So, as with prepayment medical review, fraudulent providers remain safe from investigation provided they change their tactics once "educated" about a particular practice.
- Utilization review procedures come long after payment has been made and so are useful only if there is a continuing relationship between payer and provider. The claims data forming the basis for provider profiles are usually at least 3 months old and in some cases more than 1 year old. Postpayment utilization review, therefore, comes far too late to be useful in combating the increasing number of fraud schemes run by fly-by-night operators. Storefront businesses, which fraud investigators say are increasingly prevalent, bill fast and furiously (creating extremely anomalous billing patterns) then disappear with the money long before postutilization review catches up with them. Against the threat of quick, high-volume, hit-and-run schemes, the only sure defense would be prepayment provider profiling, which would monitor each provider's aggregate billing patterns and billing acceleration rates before claims are paid. None of the sites visited had any form of prepayment provider profiling nor any prepayment method of watching for sudden surges in billings from individual providers.

Special investigative units (SIUs). The investigative units sit at the end of the referral pipeline, their cases coming from EOMB-stimulated beneficiary complaints, data-entry clerks or claims examiners, prepayment medical review, postpayment utilization review, or auditors. A small number of tip-offs from other insurers, from law enforcement agencies, or from anonymous telephone calls augment the volume of referrals.

Most investigative units work predominantly in a reactive mode, just about keeping up with the work that comes to them. Whichever mechanism produced the referrals, the investigator's job is the same: to investigate and to make cases. Following a traditional enforcement model, most of these units count their workload in terms of the number of incoming complaints or referrals and count their successes in terms of the number of cases made, settlements reached, aggregate dollars recovered, and convictions obtained.

Clearly, if the SIUs remain in a reactive mode, fed by largely ineffective referral pipelines, they will see the truth only dimly, partially, and probably very late. Without a clear focus on the goal of control—which would produce a much greater commitment to proactive outreach and intelligence gathering—SIUs can be no more effective than the referral pipelines that feed them their work.[24]

Lack of coordinated control strategy

Lack of functional coordination and the absence of any coordinating strategy further handicap fraud control efforts.[25] At each of the field sites, the simple question "Who is in charge of fraud control?" produced bafflement and responses of either "no one" or "everyone."

The development of modern claims processing systems—highly automated, high-volume, highly efficient—seems likely to exacerbate whatever functional separations already exist and to diminish even further the prospects for coherent, effective, multidisciplinary fraud control strategies.

Effects of electronic claims processing

This research also examined the impact of electronic claims processing on fraud and fraud control. Such systems exacerbate the problem of timely fraud detection. In essence, electronic claims processing creates the situation where an electronic signal received by an insurer triggers an electronic payment, often with no human intervention. The promise of administrative cost savings relies on the assumption that the majority of claims will be handled without human involvement. For fraud detection, increased speed of payment, coupled with the removal of human judgment, presents novel dangers.

One new threat involves computer-generated schemes utilizing hundreds or thousands of claims, each one carefully designed to pass through auto-adjudication to payment. Another threat involves the "quick hit" or "bust out" schemes, perpetrated by fly-by-night operators who steal millions in a relatively short period, then vanish.

Can technology provide appropriate safeguards?

Many officials express the belief that electronic claims processing systems can be made "fraud-safe" by implementing comprehensive batteries of up-front edits and audits to keep fraudulent claims out of the system altogether. If up-front preventive controls are good enough—so the theory goes—there should be less and less need for review or investigation. Many insurers are in the process of shifting resources from investigative units (labeled "reactive") into automated up-front controls (labeled "preventive"). The core of the emerging vision, therefore, could be termed *automated prevention*.

This vision, unfortunately, is fatally flawed in light of a sophisticated understanding of the fraud control challenge. It neglects the dynamic nature of the fraud control business, seriously underestimates the expertise and adaptability of the opposition, and overlooks the critical role that humans must play in any effective fraud control operation.

The vision of automated prevention assumes fraud control to be a static game; in fact, it is highly dynamic. Whatever the set of up-front controls, fraud perpetrators will quickly adjust their billing to fit. Any static set of controls only provides very temporary protection.

The vision also imagines that fraudulent claims can be distinguished from legitimate ones through analysis of the information they contain. Often they cannot. In most cases, the information content must be either compared with *other claims* to detect unusual patterns or checked against *external* information to verify its truthfulness.

However artfully constructed, automated defenses can never substitute for human common sense and will never be able to spot suspicious patterns that have not been seen before and for which they were not looking.

Automated defenses, especially when they rely mainly on "auto-rejects," provide the fraud perpetrator with complete information about what the detection systems can and cannot see. At the same time, they provide little or no opportunity for anyone *inside* the organization to gather intelligence about fraud perpetrators' latest schemes. Without a human "fraud control operation" to do the analysis, only one side in this game is gathering any useful intelligence.

Automatic rejection of claims up front is a fine tool for dealing with nonconformist billing practices or for rejecting claims containing obvious mistakes. The audience for such rejections is mostly honest and happy to be corrected. But relying on automatic up-front rejection of claims as the principal tool to fight fraud is naive. Usually, "auto-rejection" is a lame and feeble response to a new fraud threat, one that leaves the criminal perpetrator unscathed and free to try something different tomorrow.

The pervasive vision for fraud control under electronic prevention provides a diminishing (or vanishing) role for a human fraud control team. If this trend continues uncorrected, the advent of electronic claims processing will cement in place one of the major failings of fraud control systems today: no one is in charge, and no one is responsible for fraud control.

Effects of managed care

The study also briefly considered the advent of managed care and its implications for fraud and fraud control, showing that managed care will not provide a structural solution to the fraud problem, as many had hoped. Fraud will certainly take different forms under the various types of managed care contractual arrangements.

This study identified substantial difficulties law enforcement will face in dealing with managed care fraud and suggests that the criminal justice system will become less and less relevant to fraud control. At the same time, the new forms of fraud—involving diversion of capitation fees and resulting in inadequate medical care—may be more dangerous to human health than the types of fraud familiar under traditional fee-for-service arrangements.

Conclusions

Most insurers, public and private, do not systematically measure the fraud problem. They fly blind, remaining largely oblivious to the magnitude of the problem. This study failed to locate a single insurer that made resource allocation decisions based on valid estimates of the size of the problem. Massive underinvestment in fraud controls appears to be an industry norm.

Most insurers fail to designate responsibility for fraud control, and many equate it with investigation. They have no one responsible for playing the fraud control game and little prospect of effective coordination between different functional tools.

In terms of explicit strategy, many fraud units are bogged down in a reactive, case-making mode, unable to see the forest for the trees. At the other extreme, some proponents of electronic claims processing are in danger of proposing an extreme version of prevention, which threatens to eliminate human beings from the fraud control operation almost entirely, and which may decimate investigative and enforcement capacities. Insurers need a rational, integrating, control-oriented framework.

Most insurers, even if they believe in the value of proactive outreach and intelligence gathering, cannot find or protect resources for it. So they operate with a distorted and fragmentary picture of fraud, as revealed by largely ineffective detection and referral systems. And most payment systems remain vulnerable to multimillion dollar quick-hit scams because they lack the necessary prepayment controls.

Two developments are necessary before significant progress can be made in the battle against health care fraud: (1) the complexity of the fraud control challenge must be grasped and understood, and (2) the health care industry and public must learn the true extent of fraud in the American health care system. Without that knowledge, no one can justify the cost or inconvenience associated with operating appropriate controls. This study may help a little with the first. Only a commitment to systematic measurement can produce the second. Until these two developments occur, effective fraud control will most likely remain elusive.

Notes

[1] Health Care Financing Administration, *Financial Report for Fiscal Year 1996*, Washington, D.C.: U.S. Department of Health and Human Services, Health Care Financing Administration, 1997; Health Care Financing Administration, *Financial Report for Fiscal Year 1997*, Washington, D.C.: U.S. Department of Health and Human Services, Health Care Financing Administration, 1998.

[2] U.S. Department of Justice, *1997 Annual Report*, Washington, D.C.: U.S. Department of Justice, 1997: 27. The crimes included submitting false claims to Medicare, Medicaid, and other insurance plans; home health care fraud; fake billings by foreign doctors; and needless prescriptions for durable medical equipment by physicians in exchange for a kickback from manufacturers.

[3] Vladeck, B. A., "From the Health Care Financing Administration: Medicare, Medicaid Fraud and Abuse," *Journal of the American Medical Association*, 273(10)(March 8, 1995): 766.

[4] Freeh, Louis J., Director, Federal Bureau of Investigation, Statement before the Special Committee on Aging, U.S. Senate, Washington, D.C., March 21, 1995, 2.

[5] Eichenwald, K., "Unwitting Doctors and Patients Exploited in a Vast Billing Fraud," *The New York Times*, February 6, 1998, A1.

[6] Pear, R., "Medicare Contractor Admits Longtime Pattern of Fraud," *The New York Times*, July 17, 1998, A10.

[7] Jagger, Sarah F., Director, Health Financing and Policy Issues, Health, Education and Human Services Division, General Accounting Office, "Medicare and Medicaid: Opportunities to Save Program Dollars by Reducing Fraud and Abuse," testimony before the Subcommittee on Human Resources and Intergovernmental Relations, Committee on Government Reform and Oversight, House of Representatives, Washington, D.C., March 22, 1995.

[8] Ibid.

[9] Ibid.

[10] Reiss, A. J., Jr., and A. D. Biderman, "Data Sources on White-Collar Law-Breaking," Washington, D.C.: U.S. Department of Justice, National Institute of Justice, September 1980: 91.

[11] Morey, Larry, Deputy Inspector General for Investigations, Office of Inspector General, Department of Health and Human Services, statement to the Subcommittee on Health of the Committee on Ways and Means, House of Representatives. 103rd Congress, 1st Session, March 8, 1993. Serial 103–3. p. 35.

[12] Clarke, M., "The Control of Insurance Fraud: A Comparative View," *The British Journal of Criminology*, 30(1)(Winter 1990): 2.

[13] Freeh, Statement, 4.

[14] General Accounting Office, "Health Insurance: Vulnerable Payers Lose Billions to Fraud and Abuse," Report to the Chairman, Subcommittee on Human Resources and Intergovernmental Relations, Committee on Government Operations, House of Representatives, Washington, D.C., May 1992: 23.

[15] Medicare Part B is funded from general tax revenues (roughly 75 percent) and from premiums paid by the elderly. See DeLew, N., "Medicare at 30: Preparing for the Future," *Journal of the American Medical Association*, July 19, 1995: 259–267.

[16] Jagger, "Medicare and Medicaid: Opportunities to Save Program Dollars by Reducing Fraud and Abuse," 12.

[17] Clarke, "The Control of Fraud: A Comparative View," 2.

Prescription for progress

Supported by a second grant from the National Institute of Justice, Dr. Sparrow has developed and proposed a model fraud control strategy, which is described in detail in chapter 8 of his book *License to Steal* (see "Related Reading"). He recommends adoption of the following seven elements as the minimal basis for any effective fraud control operation:

1. Commitment to routine, systematic measurement of losses due to fraudulent and abusive billing practices.

2. Resource allocation for controls to be based, in some logical way, upon continuing assessment of the seriousness of the problem (that is, on the results of a measurement program).

3. Clear designation of responsibility for fraud *control* (as distinct from *investigation*) so that various contributory functions can be integrated into a strategy designed to reduce the level of fraud.

4. Adoption of a "problem solving" approach to fraud control (as a constructive way out of the strategic dilemma between reactive and preventive strategies).

5. Deliberate focus on early detection of emerging fraud problems, with consequent investments in intelligence gathering and proactive outreach.

6. Design and implementation of flexible, fraud-specific prepayment controls under the direct control of a fraud control team.

7. Adoption of a policy that every claim, no matter how small the amount and how respectable the claimant, should face some non-zero risk of random review. These random reviews should incorporate external validation of the claim, sufficient to reveal fraud if present—which would mean, at a minimum, calling patients or their relatives to verify the nature of the treatment provided.

In chapter 9 of *License to Steal*, Dr. Sparrow examines the industry's use of technology in support of fraud detection and defines the most fruitful form of future technology investments in this area.

18. Ibid., 9.

19. "EITC Compliance Study: Tax Year 1993," 5. The study was released publicly as an appendix to the Statement of Margaret Milner Richardson, Commissioner of the Internal Revenue Service, before the Subcommittee on Oversight, House Ways and Means Committee, U.S. House of Representatives, Washington, D.C., June 15, 1995.

20. Gardiner, J. A., and T. R. Lyman, *The Fraud Control Game: State Responses to Fraud and Abuse in AFDC Medicaid Programs*, Bloomington, Indiana: Indiana University Press 1984: 7.

21. Clarke, "The Control of Fraud: A Comparative View," 1.

22. Office of Management and Budget, "Analytical Perspectives: The Budget of the United States Government. Fiscal Year 1996." Executive Office of the President of the United States, Office of Management and Budget, Washington, D.C., 1995, 229.

23. Ford, J., "Health Care Fraud: The Silent Bandit," *FBI Law Enforcement Bulletin* (October 1992): 2–7.

24. General Accounting Office, "Health Insurance: Vulnerable Payers Lose Billions to Fraud and Abuse."

25. Halperin, Donald M., "A Partnership Approach: A Prescription for Enhanced Coordination of Medicaid Fraud Detection and Prevention in New York State." New York State Senate, Albany, New York, June 1993.

Malcolm K. Sparrow, M.A., M.P.A., Ph.D., is Professor of Practice at the John F. Kennedy School of Government, Harvard University. This study was supported under grant number 94–IJ–CX–K004 by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice.

The objective of the second phase of this project, also funded by NIJ, was development of a model fraud-control strategy and practical methods and tactics for improving control operations.

Findings and conclusions of the research reported here are those of the author and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

This and other NIJ publications can be found at and downloaded from the NIJ Web site (http://www.ojp.usdoj.gov/nij).

NCJ 172841

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Washington, DC 20531