

INGENIX[®]

**Using Technology to Enhance
Pre-Payment Fraud Detection:
A Multi-Dimensional Strategy**



It's difficult to accurately estimate the full financial impact of health care fraud and abuse because much of it goes unreported, or worse yet, undiscovered. Conservative estimates indicate the health care industry lost \$51 billion in 2003 to fraud, yet other estimates place the annual loss as high as \$170 billion.¹

The statistics only scratch the surface. The full financial impact of fraud and abuse cuts much deeper into the tissue of the nation's economy. Decreased profitability at health plans triggers the need to raise premiums. These higher rates raise operational costs for employers, forcing them to either increase the price of goods and services, or pass along the additional costs to employees by making them pay more for their coverage through higher co-pays and out-of-pocket expenses. In the end, consumers are financially stretched on multiple fronts, including higher insurance premiums, co-pays, and deductibles and increased prices for goods and services. As a result, it is estimated that insurance fraud ends up costing each U.S. household \$940 per year.²

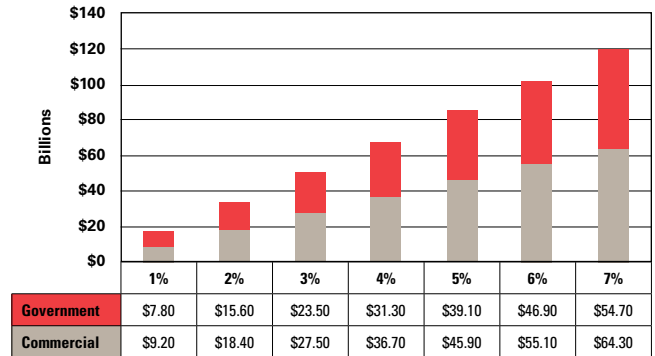
Adding further injury is the increased incidence of identity theft. Today's digital economy makes it relatively easy for individuals to receive free care by stealing or fabricating social security numbers, health insurance, and personal identification cards. These costs are absorbed by payers and ultimately passed along to employers and consumers.

All of these factors make it difficult to estimate the full financial impact of fraud and abuse, but it is clear that dramatic savings opportunities exist with even modest prevention and detection efforts. For example, anti-fraud efforts that prevent one percent of government and commercial health plan overpayments would result in \$17 billion annual savings.³ Such savings have the potential to substantially increase payer profitability. An anti-fraud program that saves one percent of medical expenses can potentially increase the profitability of a typical health plan by 16.7 percent.⁴

Prevention and Detection Challenges

Until recently, focusing on the prevention and detection of fraud and abuse has not been a priority for health plans. Part of the challenge stems from how the industry is structured. Due to claim volume, payers have developed claims

OVERPAYMENTS AS A PERCENTAGE OF PAYOUT



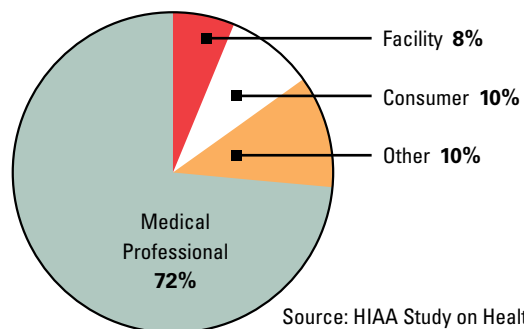
Assumptions: Commercial annual payout \$918B, Government annual payout \$782B

processing systems to process massive amounts of claims efficiently and rapidly with a focus on coding accuracy. And while states mandate prompt claim payment, they do not allow exemptions for legitimate investigations of suspicious claims. As a result, the majority of health plans have focused their spending on technology to simply keep up with the flow of claims and make efficiency improvements, rather than making investments in fraud strategies or controls.

The industry has traditionally relied upon law enforcement to control its fraud. Statistics, however, prove this approach ineffective. In 2005, there were 25,945 suspected fraud referrals made to the New York Insurance Frauds Bureau. Of those, 1,179 (4.5 percent) were opened as new cases and only 224 (0.86 percent) were pursued for prosecution.

Identifying the perpetrators is another challenge. Most fraud cases are committed by people connected to the health care industry—those with the access to information and tools to benefit from the crime. Medical professionals, health care

SUSPECTED FRAUD CASES BY TYPE OF PERPETRATOR



Source: HIAA Study on Health Care Fraud

1 "Healthcare Fraud: A Serious and Costly Reality for All Americans," National Health Care Anti-Fraud Association, October 2005, http://www.nhcaa.org/pdf/all_about_hcf.pdf.
 2 New York State Insurance Department.
 3 Assumption based on commercial annual payout of \$918 billion and government payout of \$782 billion.
 4 Reden & Anders, validated through client visits.

facilities, and consumers represent about 90 percent of the perpetrators. Although these offenders are difficult to catch and prosecute, the remaining 10 percent remain much more elusive, since they include such a broad spectrum of individuals. This segment may include insurance brokers and agents and even con artists, organized crime, drug dealers, and terrorists.

Internal fraud and abuse occurrences are partially the result of a mindset among providers that managed care practices are squeezing physician earnings, making certain providers believe that it is acceptable to “bend the truth” when submitting claims to increase profits. A study published in *The Journal of the American Medical Association* surveyed physicians and received the following responses:

- Fifty-four percent reported using deception of third-party payers to obtain benefits.
- Thirty-nine percent reported that they exaggerated a patient’s condition, changed a diagnosis, or reported signs or symptoms that didn’t exist to obtain higher reimbursement.⁵

Ultimately, unscrupulous physician practices and fabrications of medical histories have the potential to jeopardize the future insurability and employability of patients. Patients may be exposed to additional risks in instances when physicians perform unnecessary tests and procedures to gain higher reimbursement. In addition, false or inflated claims rob the system of limited dollars that are intended for the care of patients.

Proactive Approaches to Fraud and Abuse Detection

To reduce losses, the health care industry is taking a lesson from the financial services industry by no longer relying exclusively on law enforcement to solve its payment integrity issues. Instead, health plans are evolving their fraud and abuse strategies from “pay and chase” to “prevent and save,” which results in greater savings.

Effective fraud detection is best achieved through an integrated approach to claims analysis. With a retrospective (or post-payment) approach, payers can analyze historical

claims to identify patterns and trends that signify fraudulent activity. For example, retrospective peer-to-peer analysis can enable payers to identify provider organizations that consistently code encounters with complications and co-morbidities to gain higher reimbursement, which may signify fraudulent activity.

Once trends, norms, and patterns are identified using retrospective analysis, the information can be used for the prospective detection of fraud—enabling payers to identify aberrant billing patterns and pend payment of suspicious claims until the matter is investigated. Prospective detection can employ both provider-centric and claims-centric approaches.

Provider-centric detection efforts flag physicians and facilities who are known and suspected fraud perpetrators and those who are facing sanctions from state medical associations. By investigating licensure, sanctions, and addresses of all new providers, payers can identify “phantom providers” who are criminals filing claims without practicing medicine, as well as providers who are filing claims without proper licensure.

Claims-centric approaches can analyze claims in real-time to detect aberrant billing patterns, including:

- Improperly coding procedures as medically necessary, such as cosmetic procedures that are coded as a treatment of a primary diagnosis.
- Double billing of a procedure by initially submitting it in a group of bundled claims and later resubmitting it as an individual claim.
- Billing for services outside of the physician’s practice area, such as having an allergy specialist submit a claim for hip replacement procedure.
- Coding for services that are unlikely, such as a hysterectomy procedure on a male patient.

⁵ “Fidelity and Deceit at the Bedside,” M.Gregg Bloche. *The Journal of the American Medical Association*, April 2000: 283: 1881-1884.

⁶ Statistics based on Ingenix past client performance.

Successful pre-payment fraud detection efforts rely heavily on technology solutions to collect the necessary data and apply the business rules that identify suspicious activity. Properly configured, fraud-detection solutions can handle the high volume of claims that payers receive and comb through the more than 1,200 data elements contained in each claim. When applied to the entire claims stream, these solutions can boost bottom-line savings by 0.5 to one percent, which can translate into a 16 percent profitability improvement.⁶

IMPACT OF EFFECTIVE FRAUD CONTROLS

High Level Payer P&L:

	PMPM	PMPY
Revenue	\$252	\$3024
Medical Expenses	\$200	\$2400
Admin & Operating Expenses	\$40	\$480
Profit (5/6%)	\$12	\$144

Practical Applications

The success of pre-payment fraud detection efforts is largely dependent upon the efficiency and accuracy of the solutions that are employed. High rates of false positives decrease productivity as higher levels of human intervention are needed to investigate cases, and delayed reimbursement strains provider relations. The most effective solutions rely on more than generic statistical analysis to identify fraud.

APPROACHES TO FRAUD & ABUSE MANAGEMENT

Approach	Reactive	Retrospective Data Mining	Prospective	Predictive	Integrated Real-Time Detection
Characteristics	Based on tips, referrals, and random audits Staffed by ex-law enforcement	Looks for unusual payment trends Validates tips and referrals	Prospective management of claims from known suspicious providers	Prospective identification of claims that are statistically unusual (not just fraud)	Prospective management of schemes and scams based on pattern recognition
Benefits	Sentinel effect Compliance with regulatory mandates Weakness: negative or neutral ROI	Basis for recovery cases Increased number and volume of cases Positive ROI	4-5 times more effective than retrospective recovery	Increases prospective savings by another 30-50%	Applied to the entire claims stream for maximum impact Bottomline savings of .5-1% of allowed claims dollars for up to 16% payer profitability improvement

Clinical and investigative domain expertise—combined with analytical skills—are necessary to design health care-specific solutions that will deliver a high return on investment by reducing fraudulent activity.

The success of an anti-fraud program is largely dependent upon the metrics used to measure its effectiveness. A reliable metric is to measure the dollars that are never paid due to identification of fraud and abuse as a percentage of the otherwise allowable payments. In contrast, health plans should avoid other metrics that don't translate into material savings, such as the number of referrals to law enforcement, the prediction of future savings, and savings expressed as "billed dollars."

Successful fraud and abuse prevention programs provide payers with an effective cost-containment tool to gain a competitive advantage. Following years of premium increases, health plans are feeling the pressure to reduce rate increases by improving administrative efficiency. That leaves payers with the medical expense component to focus on additional cost reductions—making fraud and abuse prevention a practical approach to increase profitability.

Implementing a multidimensional, pre-payment fraud detection strategy can help health plans improve the financial health of the industry and provide affordable, quality health care to those who need it.

Ingenix | Intelligence for Health Care | www.ingenix.com

From North America, call: 1-800-765-6034 • ingenuity@ingenix.com
For a list of Ingenix global office locations, please refer to our web site.

Corporate Headquarters | 12125 Technology Drive, Eden Prairie, MN 55344

Ingenix and the Ingenix logo are registered trademarks of Ingenix, Inc. All other brand or product names are trademarks or registered marks of their respective owners. Because we are continuously improving our products and services, Ingenix reserves the right to change specifications without prior notice. Ingenix is an equal opportunity employer.

06-10349 5/07 Original © 2007 Ingenix. All Rights Reserved