Healthcare Fraud and Abuse

*by William J. Rudman, PhD; John S. Eberhardt III; William Pierce, RHIA;
and Susan Hart-Hester, PhD*

In Texas, a supplier of durable medical equipment was found guilty of five counts of healthcare fraud due to submission of false claims to Medicare. The court sentenced the supplier to 120 months of incarceration and restitution of $1.6 million.[1]

Raritan Bay Medical Center agreed to pay the government $7.5 million to settle allegations that it defrauded the Medicare program, purposely inflating charges for inpatient and outpatient care, artificially obtaining outlier payments from Medicare.[2]

AmeriGroup Illinois, Inc., fraudulently skewed enrollment into the Medicaid HMO program by refusing to register pregnant women and discouraging registration for individuals with preexisting conditions. Under the False Claims Act and the Illinois Whistleblower Reward and Protection Act, AmeriGroup paid $144 million in damages to Illinois and the U.S. government and $190 million in civil penalties.[3]

In Florida, a dermatologist was sentenced to 22 years in prison, paid $3.7 million in restitution, forfeited an addition $3.7 million, and paid a $25,000 fine for performing 3,086 medically unnecessary surgeries on 865 Medicare beneficiaries.[4]

In Florida, a physician was sentenced to 24 months incarceration, ordered to pay $727,000 in restitution for cash payments where the physician signed blank prescriptions and certificates for medical necessity for patients he never saw.[5]

The U.S. Department of Health and Human Services (HHS) Office of the Inspector General (OIG) found that providers in 8 out of 10 audited states received an estimated total of $27.3 million in Medicaid overpayments for services claimed after beneficiaries' deaths.[6]

Key words: fraud and abuse; computer assisted coding; data mining

Introduction

The above are some examples of fraud presented by the HHS and Department of Justice fraud and abuse report for 2007. It is projected that fraud and abuse account for between 3 to 15 percent of annual expenditures for healthcare in the United States. The National Healthcare Antifraud Association Report (March 2008) suggests that the cost ranges between 3 to 10 percent; the GAO 2008 and the Congressional Budget Office place the estimated cost at 10 percent; and the U.S. Chamber of Commerce Report places it at 15 percent.[7–9] Using these data as a base, the estimated cost of fraud and abuse ranges from $100–170 billion annually.

To help combat fraud and abuse, the federal government's False Claims Act (FCA) of 1986 specifically targeted healthcare fraud and abuse. Under the FCA, the United States may sue violators for treble damages, plus $5,500–11,000 per false claim. To further fight the rising incidence of fraud and abuse, in 1993 the Attorney General announced that tracking fraud and abuse would be a top priority for the Department of Justice. In 1993 the Health Insurance Portability and Accountability Act of 1996 (HIPAA) established the Health Care Fraud and Abuse Control program (HCFAC). In 2007, HHS and the Attorney General allocated $248,459,000 to HCFAC to fight healthcare fraud and abuse.

During the time period from 1997 to 2007, HCFAC collected over $11.2 billion in fraudulent claims, $1.8 billion in 2007 alone.[10] As a result of increased surveillance, HHS and OIG estimate that their efforts resulted in healthcare savings (i.e., "funds put to better use as a result of…program initiatives") of approximately $39 billion.[11]

Despite federal legislation and a commitment of millions of dollars to fight fraud and abuse, research suggests that less than 5 percent of the losses from fraud and abuse are recovered annually.[12] This paper will provide both a technical and working definition of fraud and abuse, identify the most common types of healthcare fraud and abuse, and provide a working model that uses data mining methods for detecting and managing (identifying and reducing) fraud and abuse.

What Is Healthcare Fraud?

Under HIPAA, "fraud is defined as knowingly, and willfully executes or attempts to execute a scheme…to defraud any healthcare benefit program or to obtain by means of false or fraudulent pretenses, representations, or promises any of the money or property owned by…any healthcare benefit program."[13] Abuse is most often defined in terms of acts that are inconsistent with sound medical or business practice ().[14] Unlike fraud, abuse is an unintentional practice that directly or indirectly results in an overpayment to the healthcare provider. Abuse is similar to fraud, except that the investigator cannot establish the act was committed knowingly, willfully, and intentionally.[15] Use of the term "intentional" is important in defining fraud and abuse and in identifying ethical or unethical action.[16]

Some of the most common types of fraud and abuse are misrepresentation of services with incorrect Current Procedural Terminology (CPT) codes; billing for services not rendered; altering claim forms for higher payments; falsification of information in medical record documents, such as International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM) codes and treatment histories; billing for services that were not performed or misrepresenting the types of services that were provided; billing for supplies not provided; and providing medical services that are unnecessary based on the patient's condition.

Solutions to Fraud and Abuse

Under the above definitions, it is impossible to delineate between fraud and abuse on the basis of evaluating a single case or record. In order to prove fraud, the government must prove that the acts were performed knowingly, willfully, and intentionally. To prove fraud occurred rather than abuse, the upcoding or miscoding of an event must occur over time and across a large number of patients. For example, in the case of the Florida dermatologist noted above, fraud occurred over a period of six years, 3,086 false procedures, and 865 patients.[17]

While it is impossible to stop an individual who intentionally commits fraud, there are certain external and internal systems and processes that can be implemented to better detect fraud and abuse and to deter future fraud and abuse. From our review of the literature, the following four solutions to identifying and reducing fraud and abuse are suggested:

1. Training and education
2. Implementation of computer-assisted coding (CAC)
3. Increased federal enforcement of fraud and abuse monitoring
4. Use of data modeling and data mining

Training and Education

Educational training programs focused on deterring fraud and abuse must first and foremost stress the importance of appropriate documentation and coding in accurately identifying the patient's condition in order to provide timely and effective care. Accurate medical record documentation is essential not only in addressing issues of fraud and abuse but in providing patients with quality care. These educational training sessions must emphasize the accuracy of the coding in order to ensure that undercoding as a result of the physician's fearing repercussions of overcoding does not occur. One study found that undercoding was three times more likely to occur than overcoding.[18, 19] Training sessions should not focus on overcoding or undercoding but on providing the appropriate documentation to support the code. Documentation must be directly tied to the patient's condition and services required to treat the condition.

Evaluation and management (E&M) CPT codes seem to be one area where documentation and coding issues are prevalent. Educational and training programs focused on CPT codes should emphasize the importance of documentation to support time spent examining the patient. There are five levels of E&M coding, ranging from 99201 to 99205. Each level requires more specification in documentation to justify reimbursement levels based on the expected amount of time the physician spends with the patient to perform services required. For example, a Level 1 code (99201) is usually used for patients with minor problems, where the history and examination are focused and medical decision making is straightforward. Typically, for a Level 1 code, the physician would spend approximately 10 minutes face-to-face with the patient. For a Level 3 code (99203), the presenting problems are low to moderate in severity, and the history and examination is more detailed; however, the medical decision making is likely to be of low complexity. Here the physician would typically spend approximately 30 minutes face-to-face with the patient. To avoid charges of fraud or abuse, the physician must justify through documentation the additional 20 minutes spent in face-to-face care to receive the higher reimbursement level.

Implementation of fraud and abuse education and training programs may be facilitated through establishing corporate or staff coding committees to create standards and protocols (e.g., standard abbreviations, documentation for medical necessity). This committee would consist of a compliance officer, health information management (HIM) staff, physicians, nurses, and financial administrators. The coding committee would establish guidelines for staff concerning proper documentation for level of services provided, establish enterprise-wide training guidelines, perform audits to verify accuracy, and serve as a communication liaison between coders and organizational administration. The coding committee would facilitate site review of training programs focused on teaching ethical principles (such as a code of ethics) and values to providers, staff, and healthcare administrators.

In addition to establishing a coding committee, it is important to bring in external experts to provide an unbiased evaluation of guidelines and processes. Training grassroots coders through externally sponsored programs also allows HIM coders to better identify gaps in documentation related to appropriate codes. One such program is AHIMA's sponsorship of coding round tables that bring together coders from across the nation for discussion specifically focused on fraud and abuse.

Implementation of Computer-Assisted Coding

Computer-assisted coding is defined as "the use of computer software that automatically generates a set of medical codes for review, validation, and use based upon clinical documentation of the healthcare practitioner."[20] CAC tools are based on natural-language processing algorithms that automate the assignment of codes (ICD-9-CM, CPT, and Healthcare Common Procedural Coding System [HCPCS]) from clinical documentation provided by clinical staff. Currently, there are two key financial issues driving CAC adoption: 1) healthcare reimbursement and 2) compliance with anti–fraud and abuse regulations. CAC provides healthcare organizations and providers with a mechanism to reduce potential issues of fraud and abuse in medical coding. Building upon a health information technology platform, certified CAC software provides coding that is based upon standard coding principles and guidelines.[21] CAC software provides prompts and decision-support tools that assist healthcare entities and providers in completing accurate and timely supportive documentation required for specified levels of care. The implementation of CAC within the healthcare environment fosters system integrity through increased compliance with identified standards and protocols, further reducing miscoded claim submissions. Current innovations in CAC now include software that can read free text, extract information from the record, and assign the appropriate code. CAC software can be used to create an audit trail that will provide postpayment audits to detect coding errors and fraudulent practices over time.

Increased Federal Enforcement of Fraud and Abuse Monitoring

One of the most effective ways of controlling fraud and abuse is through reinforcement of federal penalties. In 2007, HHS and OIG committed approximately $248 million in the fight against fraud and abuse. This unprecedented effort resulted in a significant increase in the number of cases prosecuted, amount of money recovered, and the dollar amount of claims filed. In 2007, the U.S. Attorney's Office opened 878 new criminal fraud investigations and filed 434 new cases. During fiscal year 2007, 560 defendants were convicted of healthcare fraud related crimes. To put this in perspective, during 1988 and 2000, the federal government recovered approximately $2 billion from healthcare providers who committed fraud. In 2007, the federal government recovered slightly over $1.8 billion from healthcare providers who committed fraud. Interestingly, during the investigatory phase of the Medicare Fraud Strike Force (March 1 through September 30, 2007) submitted claims to Medicare dropped $1.2 billion from $1.87 billion to $661 million during March 1 through September 30, 2006. Furthermore, claims paid from March 1 through September 30, 2007, dropped from $485 million to $230 million over the same seven-month period during 2006.[22]

Use of Data Modeling and Data Mining

As noted above, fraud and abuse often involves multiple actors committing subtle acts over a long period of time. Fraud often involves complex patterns of very minute indicators collected over a long period of time. In a modern claims environment, with petabyte databases and limited resources for analyzing them, detecting these patterns is extremely difficult. Thus, fraud detection is usually managed by very experienced investigators who concentrate only on the largest cases because of resource constraints. Even so, most of these cases come to light only because the offender becomes greedy or makes a mistake or due to coincidence.

Data modeling and mining techniques are perhaps the most valuable tool the organization can utilize in detecting fraud and abuse. Data modeling and mining techniques can be used to identify both consumer fraud and provider fraud. Both types of fraud can cost healthcare organizations millions of dollars each year. The advancement of data mining and machine-learning programs gives healthcare organizations and providers the ability to predict potential fraud and abuse. Automated data mining technologies allow the organization to gain valuable insights and to detect patterns within data without predetermined bias. Statistical algorithms can be used to identify general trends or patterns of suspicious transactions in healthcare data sets.

In order to better explain the use of data mining and machine learning technologies in understanding fraud and abuse, the following example is offered. For purposes of this paper, we will focus on consumer fraud and abuse rather than provider fraud and abuse. Provider fraud and abuse is extremely complicated and involves numerous variables related to CPT codes, time, documentation patterns, and multiple stakeholders. This type of analysis is beyond the scope of this paper, which aims to provide a simple explanation of how data mining and modeling algorithms can be used to identify patterns of fraud and abuse.

Use of Data Mining in Analyzing and Detecting Fraud and Abuse

Given the complexity of the problem and the challenge at hand, most payers have historically used a "threshold" approach to claims review and fraud detection in which a claim or payee gets referred for review when the dollar amount or number claimed exceeds a certain threshold that has been historically observed to correlate with fraud and abuse. This is a blunt instrument: a great deal of fraud and abuse cases are too small to trigger these thresholds, many legitimate claims that are simply large are reviewed unnecessarily, and most fraud occurs over long time periods. As a result, only a small portion of fraud is actually detected (3 to 5 percent), and it is typically detected late in the cycle, resulting in only a small recovery and wasted resources that could have been used to provide care.

Data mining techniques have allowed payers to use more sophisticated techniques such as data mining, reporting, and rules engines for fraud and abuse detection. An effective automated review and detection system has three key components: 1) a data curation (organization) component, 2) an algorithmic component, and 3) an implementation process.

The first component, data curation, is focused on the development of appropriate data standards and methodologies. These include identifying source data for study and structuring data for analysis, as well as data cleaning and normalization. Issues faced in curation include the following: Where do I source my study data? Is it an appropriate representation of my population? Do I have the appropriate data elements, and do I have enough resources to collect additional elements if I need them? How do I go about cleaning entry errors? Are my outcomes properly described in my data? One of the greatest challenges in curating data for data mining is semantic normalization. If I have an orange sphere, it can be a fruit, a tennis ball, or a candy (among other things), so which is it? The best way to approach data curation is to begin a dialogue with the acknowledged domain experts, such as the investigators, to better understand what constitutes a discrete outcome, what elements constitute it, and what constitutes “success” in terms of detection. All of these should be clearly and extensively documented into a data specification, which can be based upon existing data documentation or created from scratch.

The second component, data mining and classification algorithms, requires the input of experts in data mining and statistics. Many methods can be used to develop an algorithm or set of rules for detecting fraud and abuse: Bayesian belief networks, neural networks, fuzzy logic, genetic algorithms, logistic regression, and others. People often have strong views about which method is appropriate, and entire books have been dedicated to this topic. Rather than recommend a method or algorithmic approach, we will suggest some criteria that should be considered when selecting a methodology. First, is the method appropriate to your data? Different types of algorithms are suited to different types of problems. Is your problem set linear or nonlinear? Is the outcome discrete or continuous? Second, you need to identify a method you are comfortable with. To use and trust one of these complex technologies, you must have a basic understanding of it. Different methods have different degrees of transparency—the more transparent a method, the easier it is to “gut check” the result. Third, will the method scale? You need to ensure that the method and technology you select can scale to the amount of data you will be examining. Methodology selection needs to be considered in a thoughtful and open-minded way.

The third and final component is implementation and deployment. Proper implementation and deployment consists of four critical elements: validation, system implementation, maintenance, and policy. Validation methodologies are used to ensure data are robust. These methodologies include cross-validation, interset validation, and prospective study. Implementation refers to the systems, manual or automated, that will be used to reduce the findings to practice. Implementation of coding or rules needs to be engineered and documented, with attention paid to the current workflow and with the goal of improving the workflow. Systems that derive rules from large, complex systems are already dated the moment they are turned on. This is particularly true of systems designed to detect fraud and abuse, where an adversary is actively seeking to evade detection. It is important to have a plan to maintain the system and periodically update the logic and revalidate the system’s efficacy. Finally, policy is an often overlooked element of system implementation and deployment. The same rule can often be applied in many different ways: to optimize detection, minimize false positives, or maximize accuracy. The correct implementation is a function of the relative cost (monetary and otherwise) of fraud and abuse, investigation, and false positives. While data mining can dramatically improve detection, management still has to decide what the “optimal” outcome should be so that the system can be properly tuned. Algorithms do not absolve us from decision making.

To illustrate the principles discussed above, we have developed a system using one of the data mining methods discussed above: Bayesian belief networks. This example uses artificial data since actual data has many legal and policy constraints on disclosure, and it provides a simple but easily understandable approximation of a payer environment. In our example, the algorithm is built using a simplified data set that has a selection of inpatient and outpatient diagnoses, treatment intervals, information about changing physicians, total claims, comorbidities, and our outcome of interest—fraud.

To begin with, let us briefly discuss our data mining methodology. A Bayesian belief network (BBN) is a directed, acyclic graph of conditional dependence. A BBN allows us to estimate the likelihood of a given outcome of interest given prior knowledge. Further, the manner in which this estimate is derived is through a directed (structured) network of conditional dependence (joint probability) that actually provides us with a hierarchy of information: *if I want to estimate the likelihood of A, the most useful pieces of a priori knowledge are C, D, and L*. This allows us to be efficient and only use those pieces of information that are most useful in solving the problem at hand. The BBN discussed in this example was constructed using machine learning, meaning that a computer algorithm was used to study a data set of prior evidence in order to discover the optimal structure of the BBN. Machine learning is a highly efficient method to discover rule sets in highly complex, otherwise impenetrable data sets.

The network in Figure 1 represents our example data set. We can learn several things just from the network structure itself. For example, if we want to detect fraud in our study population, the four most important factors are whether the enrollee has changed clinicians between visits, what the diagnosis is at the third outpatient visit, what the interval between second and third outpatient visits is, and what the interval between the first and second inpatient visits is.

Having observed the information structure of our population, we can dig deeper to begin to understand the evidence underlying the model and derive the rule sets that predict fraud. Figure 2 shows, with the network nodes expanded to histograms, the reference distributions of our study population. We can observe, for instance, that about 10 percent of enrollees have been involved in some type of fraud, while only about 11 percent of enrollees have changed physicians. These two features are conditionally dependent—but how do they impact one another?

In Figure 3, we input evidence into our network to understand its impact on the posterior probabilities of other features in our network. In this instance, we now know (100 percent probability) that the enrollee in question has not used the same physician for all visits. The posterior probability of fraud is now about 79 percent (compared to about 10 percent in the overall population). In addition, if we reverse the evidence and ask how many enrollees committing fraud change physicians, the answer is an estimated 90 percent. From this we can draw an inference: 79 percent of enrollees who changed physicians commit fraud, and 90 percent of enrollees who commit fraud change physicians.

Figure 4 provides data only on those who committed fraud. This provides a direct examination of characteristics of those who commit fraud. Here, we find that on the third visit (63.07%) the patient who committed fraud saw a different physician (90.2 percent). Furthermore, the visit was for pain (63.07 percent).

However, the BBN is a nonlinear model, meaning it can represent complex relationships that may have multiple solutions. In Figure 5, we examine the likelihood of fraud if a patient changes physicians but only has a single inpatient and two outpatient visits. In this case, the posterior probability of fraud drops to about 39 percent, still significantly more than the general population but significantly lower than the 79 percent estimate we receive with only the one piece of evidence.

The models allow us to codify large rule sets. For example, if we take only the four nodes most closely associated with fraud in this model and run an inference table (a table representing all possible combinations), the total number of potential rules is 216, even from this relatively simply network. Since that is too many rules to discuss here, we have selected a discrete example in Table 1, Table 2, and Table 3. In these tables, we select only two rules, where we examine an enrollee with short encounter intervals for injury—which typically has a low likelihood of fraud and abuse. However, if the enrollee changes physicians during the course of treatment, the probability of fraud increases to 53 percent. If we increase the outpatient interval to 180 days, however, the likelihood of fraud decreases to about 21 percent, perhaps reflecting that if you return to the same hospital six months later you are likely to be assigned a different attending physician.

The examination of these rules brings us to the policy question. At what predicted probability of fraud do we take action? This is a significant question because the probability threshold we select will impact whether the system is optimized toward sensitivity (detection) or specificity (accuracy). Figure 6 shows a receiver operating characteristic (ROC) curve for our fraud model. By examining Figure 6 and focusing on the crosshairs, we see that using a threshold of 12.6 percent provides a sensitivity of almost 70 percent, detecting more than two-thirds of all fraud; however, our accuracy is poor (19 percent false positives), and we get two false positives for each real case of fraud we detect. In Figure 7, we select a threshold of 40 percent and optimize toward accuracy (1 percent false positives) with very few false positives, but we only detect 60 percent of fraud. Does the value of detecting the incremental 10 percent of fraud pay for the cost of reviewing large numbers of false positives?

Finally, once our network is developed, validated, and optimized, we can deploy our rule sets, either by using the classifier in real time through batch inference or by selecting specific rule sets for implantation in systems or workflow.

Overcoming Physician Resistance to Use of Data Mining

A major concern physicians have in the use of data modeling and mining techniques is that they will be unfairly accused of fraud. A primary advantage of the data mining approach is that the resulting algorithms can be tested, validated, and optimized to an optimal level of sensitivity and specificity that will exclude patterns of normal use. Educating physicians to understand that data modeling and mining will help alleviate suspicion of fraud and abuse should go a long way to addressing their concerns.

Conclusion

In order to adequately address issues of fraud and abuse, responsibility, ownership, and consequences for actions must cross the continuum at the individual physician, healthcare provider, organizational, and federal levels. Providers as well as consumers must be committed to providing appropriate documentation to address abuse issues and take a moral and ethical stand against fraud in the healthcare environment. This may mean taking advantage of the FCA whistleblower laws to identify fraudulent claims to the appropriate federal authorities. Healthcare providers and organizations must invest in offering education and training programs, creating coding and fraud and abuse committees, and utilizing data mining and modeling software. Finally, the federal government must be diligent in prosecuting providers, healthcare organizations, manufacturers/retailers, and individuals who commit fraud and abuse in an organized and systematic manner.

William J. Rudman, PhD, is program director of the AHIMA Foundation Policy and Research Institute and a professor in the School of Medicine at the University of Mississippi Medical Center in Jackson, MS.

John S. Eberhardt III is an executive vice president and founder at DecisionQ Corporation in Washington, DC.

William Pierce, RHIA, is a systems analyst at the University of Mississippi Medical Center and works in the Center for Health Informatics and Patient Safety at the Mississippi Institute for the Improvement of Geographic and Minority Health in Jackson, MS.

Susan Hart-Hester, PhD, is a professor in the Department of Family Medicine of the School of Medicine at the University of Mississippi Medical Center in Jackson, MS, and the director of the Center for Health Informatics and Patient Safety at the Mississippi Institute for the Improvement of Geographic and Minority Health in Jackson, MS.

Notes

1. U.S. Department of Health and Human Services and Department of Justice. *Health Care Fraud and Abuse Control Program Annual Report for FY 2007* (2008). Available at http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2007.pdf.
2. Ibid.
3. Ibid.
4. Ibid.
5. Ibid.
6. Ibid.
7. National Healthcare Antifraud Association Report (March 2008)
8. GAO 2008 and the Congressional Budget Office. Testimony before the Committee on Homeland Security and Governmental Affairs Statement of Gene L. Dodaro. Available at http://www.gao.gov/new.items/d09453t.pdf.
9. U.S. Chamber of Commerce Report. Available at http://www.usdoj.gov/usao/vaw/health_care_fraud/index.html.
10. U.S. Department of Health and Human Services and Department of Justice. *Health Care Fraud and Abuse Control Program Annual Report for FY 2007* (2008). Available at http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2007.pdf.
11. Ibid, p. 25.
12. U.S. Department of Health and Human Services and Department of Justice. *Health Care Fraud and Abuse Control Program Annual Report for FY 2007* (2008). Available at http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2007.pdf.
13. Health Insurance Portability and Accountability Act 1996 (18 U.S.C., ch. 63, sec.1347).
14. Mercy Health Plans, 2009. Available at http://www.mercyhospitalplans.com/about/fraudandabuse.aspx.
15. Fraud Hotline, 2009. http://www.ssa.gov/oig/hotline/index.htm.
16. Harman, Laurinda. *Ethical Challenges in the Management of Health Information*. Second Edition (2006) AHIMA Publications.
17. U.S. Department of Health and Human Services and Department of Justice. *Health Care Fraud and Abuse Control Program Annual Report for FY 2007*.
18. Rudman, W.J. (1998) “Implementation of Outcomes Measures and Statistical Process Control Methodologies in Quality Assurance and Utilization Review Efforts within Health Information Management Departments,” *Topics in Health Information Management* (18/3): 1-7.
19. Rudman, W.J. and Hewitt, C. (November 2000) “Use of Statistical Analysis in Assessing Appropriate Documentation and Coding” *Topics in Health Information Management* (21,2):
20. AHIMA e-HIM Work Group on Computer-Assisted Coding. “Delving into Computer-assisted Coding” (AHIMA Practice Brief). *Journal of AHIMA* 75, no. 10 (November–December 2004): 48A–H.
21. Garvin, J. H., V. Watzlaf, and S. Moeini. “Automated Coding Software: Development and Use to Enhance Anti-Fraud Activities.” *AMIA 2006 Symposium Proceedings* (2006): 927. Available at http://www.pubmedcentral.nih.gov/picrender.fcgi?artid=1839655&blobtype=pdf.
22. U.S. Department of Health and Human Services and Department of Justice. *Health Care Fraud and Abuse Control Program Annual Report for FY 2007* (2008). Available at http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2007.pdf.

References

Fraud

Geis, G., P. Jesilow, H. Pontell, and M. J. O'Brien. "Fraud and Abuse of Government Medical Benefit Programs by Psychiatrists." *American Journal of Psychiatry* 142 (1985): 231–34. Available at http://ajp.psychiatryonline.org/cgi/content/abstract/142/2/231.

Morrison, James, and Theodore Morrison. "Psychiatrists Disciplined by a State Medical Board." *American Journal of Psychiatry* 158 (2001): 474–78. Available at http://ajp.psychiatryonline.org/cgi/reprint/158/3/474.

Klein, Roger D., and Sheldon Campbell. "Health Care Fraud and Abuse Laws." *Archives of Pathology and Laboratory Medicine* 130 (August 2006). Available at http://arpa.allenpress.com/pdfserv/10.1043%2F1543-2165(2006)130%5B1169:HCFAAL%5D2.0.CO%3B2.

McCall, Nelda, Harriet L. Komisar, Andrew Petersons, and Stanley Moore. "Medicare Home Health Before and After the BBA." *Health Affairs*, May/June 2001. Available at http://content.healthaffairs.org/cgi/reprint/20/3/189.

Iglehart, John K. "The Centers for Medicare and Medicaid Services." *New England Journal of Medicine* 345, no. 26 (2001, December 27): 1920–24. Available at http://content.nejm.org/cgi/content/full/345/26/1920.

Levit, Katharine, Cathy Cowan, Helen Lazenby, Arthur Sensenig, Patricia McDonnell, Jean Stiller, Anne Martin, and the Health Accounts Team. "Health Spending in 1998: Signals of Change." *Health Affairs* 19, no. 1 (2000): 124–32. Available at http://healthaff.highwire.org/cgi/reprint/19/1/124.

Kalb, Paul E. "Health Care Fraud and Abuse." *Journal of the American Medical Association* 282 (1999): 1163–68. Available at http://jama.ama-assn.org/cgi/content/abstract/282/12/1163.

Wynia, Matthew K., Deborah S. Cummins, Jonathan B. VanGeest, et al. "Physician Manipulation of Reimbursement Rules for Patients: Between a Rock and a Hard Place." *Journal of the American Medical Association* 283, no. 14 (April 12, 2000): 1858–65. Available at http://jama.ama-assn.org/cgi/reprint/283/14/1858.

Murkofsky, Rachel L., Russell S. Phillips, Ellen P. McCarthy, Roger B. Davis, and Mary Beth Hamel. "Length of Stay in Home Care Before and After the 1997 Balanced Budget Act." *Journal of the American Medical Association 289, no. 21* (June 4, 2003): 2841–48. Available at http://jama.ama-assn.org/cgi/reprint/289/21/2841.

Grogan, Colleen M., Roger D. Feldman, John A. Nyman, and Janet Shapiro. "How Will We Use Clinical Guidelines? The Experience of Medicare Carriers." *Journal of Health Politics, Policy and Law* 19, no. 1 (Spring 1994): 7–26. Available at http://jhppl.dukejournals.org/cgi/reprint/19/1/7.

Jacobson, Peter D. "Regulating Health Care: From Self-Regulation to Self-Regulation?" *Journal of Health Politics, Policy and Law* 26, No. 5 (October 2001): 1165–78. Available at http://jhppl.dukejournals.org/cgi/reprint/26/5/1165.

KPMG FORENSIC. *Fraud Survey 2003.* Available at http://kworld.com/aci/docs/surveys/Fraud%20Survey_040855_R5.pdf.

Pontell, H. N., P. D. Jesilow, and G. Geis. "Practitioner Fraud and Abuse in Medical Benefits Programs: Government Regulation and Professional White Collar Crime." *Law & Policy* 6 (1984): 405. Available at http://scholar.google.com/scholar?hl=en&lr=&q=info:4G3wIO7CmnQJ:scholar.google.com/&output=viewport&pg=1.

Blanchard, T. P. "Medicare Medical Necessity Determinations Revisited: Abuse of Discretion and Abuse of Process in the War against Medicare Fraud and Abuse." *St. Louis University Law Journal* 43 (1999): 91. Available at http://scholar.google.com/scholar?hl=en&lr=&q=info:B3Sb6KbzVugJ:scholar.google.com/&output=viewport&pg=1.

Pies, H. E. "Control of Fraud and Abuse in Medicare and Medicaid." *American Journal of Law & Medicine* 3 (1977): 323. Available at http://scholar.google.com/scholar?hl=en&lr=&q=info:f_HBBkf-6KUJ:scholar.google.com/&output=viewport&pg=1.

Lee, B. G. "Fraud and Abuse in Medicare and Medicaid." *Administrative Law Review* 30 (1978): 1. Available at http://scholar.google.com/scholar?hl=en&lr=&q=info:n3DBT2B_5EkJ:scholar.google.cm/&output=viewport&pg=1.

Davies, S. L., and T. S. Jost. "Managed Care: Placebo or Wonder Drug for Health Care Fraud and Abuse?" *Georgia Law Review* 31 (1996): 373. Available at http://scholar.google.com/scholar?hl=en&lr=&q=info:ZHG8Mbs6uu4J:scholar.google.com/&output=viewport&pg=1.

Smith, Russell G. "Fraud and Financial Abuse of Older Persons." *Australian Institute of Criminology*, no. 132, October 1999.

Bloche, M. Gregg. "Cutting Waste and Keeping Faith." *Annals of Internal Medicine* 128, no. 8 (1998): 688–89. Available at http://www.annals.org/cgi/content/full/128/8/688.

Pitches, D., A. Burls, and A. Fry-Smith. "Snakes, Ladders, and Spin—How to Make a Silk Purse from a Sow's Ear—a Comprehensive Review of Strategies to Optimise Data for Corrupt Managers and Incompetent Clinicians." *British Medical Journal* 327 (December 20, 2003): 1436–39. Available at http://www.bmj.com/cgi/content/short/327/7429/1436.

Gosfield, A. G. "The Hidden Costs of Free Lunches: Fraud and Abuse in Physician-Pharmaceutical Arrangements." *Medical Practice Management*, March/April 2005, 253–58. Available at http://www.gosfield.com/PDF/Mar_Apr_2005.MPM.pdf.

Sparrow, M. K. *License to Steal: Why Fraud Plagues America's Health Care System*. Boulder, CO: Westview Press, 1996.

Sparrow, M. K. "Fraud Control in the Health Care Industry: Assessing the State of the Art." *National Institute of Justice Research in Brief*, December 1998, 1–11. Available at http://www.ncjrs.gov/pdffiles1/172841.pdf.

Michael, J. E. "What Home Healthcare Nurses Should Know about Fraud and Abuse." *Home Healthcare Nurse* 21, no. 8 (August 2003).

Penalty

Morrison, James, and Peter Wickersham. "Physicians Disciplined by a State Medical Board." *Journal of the American Medical Association* 279, no. 23 (1998): 1889–93. Available at http://jama.ama-assn.org/cgi/reprint/279/23/1889.

Faddick, C. M. "Health Care Fraud and Abuse: New Weapons, New Penalties, and New Fears for Providers Created by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)." *Annals of Health Law* 6 (1997): 77. Available at http://scholar.google.com/scholar?hl=en&lr=&q=info:PGag905_83gJ:scholar.google.com/&output=viewport&pg=1.

Coding

Kassirer, Jerome P., and Marcia Angell. "Evaluation and Management Guidelines—Fatally Flawed." *New England Journal of Medicine* 339, no. 23 (December 3, 1998): 1697–98. Available at http://content.nejm.org/cgi/content/full/339/23/1697.

Brett, Allan S. "New Guidelines for Coding Physicians' Services—A Step Backward." *New England Journal of Medicine* 339, no. 23 (December 3, 1998): 1705–8. Available at http://content.nejm.org/cgi/content/full/339/23/1705.

Phillips, C. D., and B. J. Hillman. "Coding and Reimbursement Issues for the Radiologist." *Radiology* 220, no. 1 (2001): 7. Available at http://radiology.rsnajnls.org/cgi/reprint/220/1/7.

Shane, R. "Detecting and Preventing Health Care Fraud and Abuse—We've Only Just Begun." *American Journal of Health-System Pharmacy* 57, no. 11 (2000): 1078. Available at http://www.ajhp.org/cgi/reprint/57/11/1078.

Malatestinic, W., L. A. Braun, J. A. Jorgenson, and J. Eskew. "Components of Medicare Reimbursement." *American Journal of Health-System Pharmacy* 60, suppl. 6 (November 1, 2003). Available at http://www.ajhp.org/cgi/reprint/60/suppl_6/S3.pdf.

Hand, R. W. "E&M Guidelines." *Chest* 113 (1998): 1432–34. Available at http://www.chestjournal.org/content/113/6/1432.full.pdf+html.

King, M. S., L. Sharp, and M. S. Lipsky. “Accuracy of CPT Evaluation and Management Coding by Family Physicians.” *Journal of the American Board of Family Medicine* 14, no. 3 (2001): 184. Available at http://www.jabfm.com/cgi/reprint/14/3/184.

Chute, C. G. “Clinical Classification and Terminology—Some History and Current Observations.” *Journal of the American Medical Informatics Association* 7 (2000): 298–303. Available at http://www.jamia.org/cgi/content/abstract/7/3/298.

Gruber, N. P., H. Shepherd, and R. V. Varner. “Role of a Medical Staff Coding Committee in Documentation, Coding, and Billing Compliance*.” Psychiatric Services* 53, no. 12 (2002): 1629. Available at http://www.psychservices.psychiatryonline.org/cgi/reprint/53/12/1629.

Adams, D. L., H. Norman, and V. J. Burroughs. “Addressing Medical Coding and Billing Part II: A Strategy for Achieving Compliance. A Risk Management Approach for Reducing Coding and Billing Errors.” *Journal of the National Medical Association* 94, no. 6 (June 2002): 430–47. Available at http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2594405.

Lorence, D. P., and A. Spink. “Regional Variation in Medical Systems Data: Influences on Upcoding.” *Journal of Medical Systems* 26, no. 5 (October 2002): 369–81. Available at http://www.springerlink.com/content/d83b53h5gdjye65n/fulltext.pdf.

Software

Phua, C., V. Lee, K. Smith, and R. Gayler. “A Comprehensive Survey of Data Mining-based Fraud Detection Research.” Available at http://clifton.phua.googlepages.com/fraud-detection-survey.pdf.

Fried, B. M., G. Weinrelch, G. M. Cavalier, and K. J. Lester. “E-Health: Technologic Revolution Meets Regulatory Constraint.” *Health Affairs*, November/December 2000. Available at http://healthaff.highwire.org/cgi/reprint/19/6/124.pdf.

Jiang, Y., M. Nossal, and P. Resnik. “How Does the System Know It’s Right? Automated Confidence Assessment for Compliant Coding.” *Perspectives in Health Information Management*. CAC Proceedings, Fall 2006. Available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_032075.pdf.

Heinze, D. T., M. I. Morsch, R. E. Sheffer, M. A. Jimmink, M. A. Jennings, W. C. Morris, and A. E. Morsch. “LifeCode—A Deployed Application for Automated Medical Coding.” *AI Magazine* 22, no. 2 (2001). Available at http://www.aaai.org/ojs/index.php/aimagazine/article/viewFile/1562/1461.

Hankin, R. A. “BarCoding in Healthcare—A Critical Solution.” *Business Briefing: Medical Device Manufacturing & Technology* (2002). Available at http://www.hibcc-au.com.au/Reference%20Files/Hankin_pap.pdf.

Ortega, P. A., C. J. Figueroa, and G. A. Ruz. “A Medical Claim Fraud/Abuse Detection System based on Data Mining: A Case Study in Chile.” Available at http://www.mec.cf.ac.uk/~scegr2/pub/DMI5560.pdf.

Sojol, L., B. Garcia, J. Rodriguez, M. West, and K. Johnson. “Using Data Mining to Find Fraud in HCFA Health Care Claims.” *Topics in Health Information Management*22, no. 1 (August 2001): 1–13. Available at http://www.ncbi.nlm.nih.gov/pubmed/11680273.

Yang, W., and S. Hwang. “A Process-Mining Framework for the Detection of Healthcare Fraud and Abuse.” *Expert Systems with Applications* 31, no. 1 (July 2006): 56–68. Available at http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V03-4H74XHS-1&_user=479005&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000022959&_version=1&_urlVersion=0&_userid=479005&md5=58ef1374b9ee4338a1c0a284a14d7251.

Woodfield, T. J. “Predicting Workers’ Compensation Insurance Fraud Using SAS Enterprise Miner 5.1 and SAS Text Miner.” SAS Institute white paper (071-30). Available at http://www2.sas.com/proceedings/sugi30/071-30.pdf.

Legal/Law

Klein, R. D., and S. Campbell. “Health Care Fraud and Abuse Laws.” *Archives of Pathology and Laboratory Medicine* 130 (August 2006): 1169–77. Available at http://arpa.allenpress.com/pdfserv/10.1043%2F1543-2165(2006)130%5B1169:HCFAAL%5D2.0.CO%3B2.

Blumstein, J. F. “Rationalizing the Fraud and Abuse Statue.” *Health Affairs* 15, no. 4 (Winter 1996): 118. Available at http://content.healthaffairs.org/cgi/reprint/15/4/118.

Stanton, T. H. “Fraud and Abuse Enforcement in Medicare: Finding Middle Ground.” *Health Affairs* 20, no. 4 (2001): 28. Available at http://content.healthaffairs.org/cgi/reprint/20/4/28.

Blumstein, J. F. “The Fraud and Abuse Statute in an Evolving Health Care Marketplace: Life in the Health Care Speakeasy.” *American Journal of Law & Medicine* 22 (1996): 205. Available at http://scholar.google.com/scholar?hl=en&lr=&q=info:kLN_Up_YkXkJ:scholar.google.com/&output=viewport&pg=1.

Glauser, J. “The False Claims Act Rewards Greed, Not Honest Attempts to Comply with Coding Guidelines.” *Emergency Medicine News* 24, no. 5 (May 2002): 26, 28. Available at http://www.em-news.com/pt/re/emmednews/fulltext.00132981-200205000-00018.htm;jsessionid=KWrJfRtYVmGrMRNnlxWG8hpxnGmhJjFCpmpwMlP7bWq6NVBCnyJv!-1775402713!181195628!8091!-1.

Jesilow, P. D., P. N. Pontell, and G. Geis. “Medical Criminals: Physicians and White-Collar Offenses.” *Justice Quarterly* 2, no. 2 (June 1985): 149–65. Available at http://www.informaworld.com/smpp/content~content=a718864848~db=all.

Hyman, D. A. “Health Care Fraud and Abuse: Market Change, Social Norms, and the Trust ‘Reposed in the Workmen.’” *Journal of Legal Studies* 30 (June 2001). Available at http://www.journals.uchicago.edu/doi/abs/10.1086/324674.

Barrett, M. K., and B. A. Liang. “The Rules of Fraud and Abuse.” *Hematology/Oncology Clinics of North America* 16, no. 6 (December 2002). Available at http://www.mdconsult.com/das/article/body/138958743-2/jorg=journal&source=&sp=12607092&sid=0/N/319836/1.html?issn=0889-8588.

Buppert, C. “Avoiding Medicare Fraud Part 1.” *Nurse Practitioner* 26, no. 1 (January 2001): 70, 72–75.

Buppert, C. “Avoiding Medicare Fraud Part 2.” *Nurse Practitioner* 26, no. 2 (February 2001): 34–38.

Figure 1

Bayesian Belief Network of Healthcare Claims Fraud

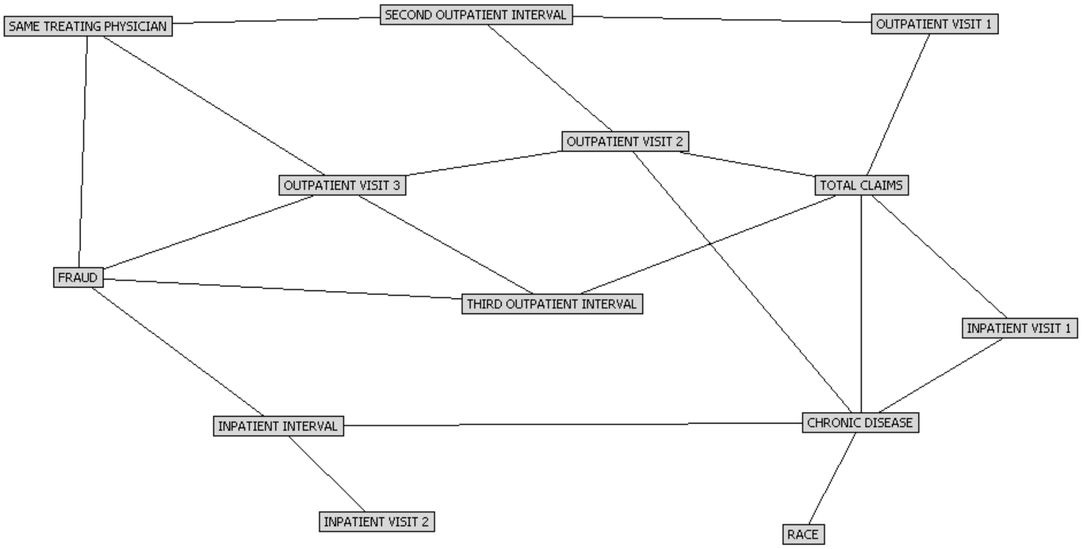


Figure 2

Reference Distributions

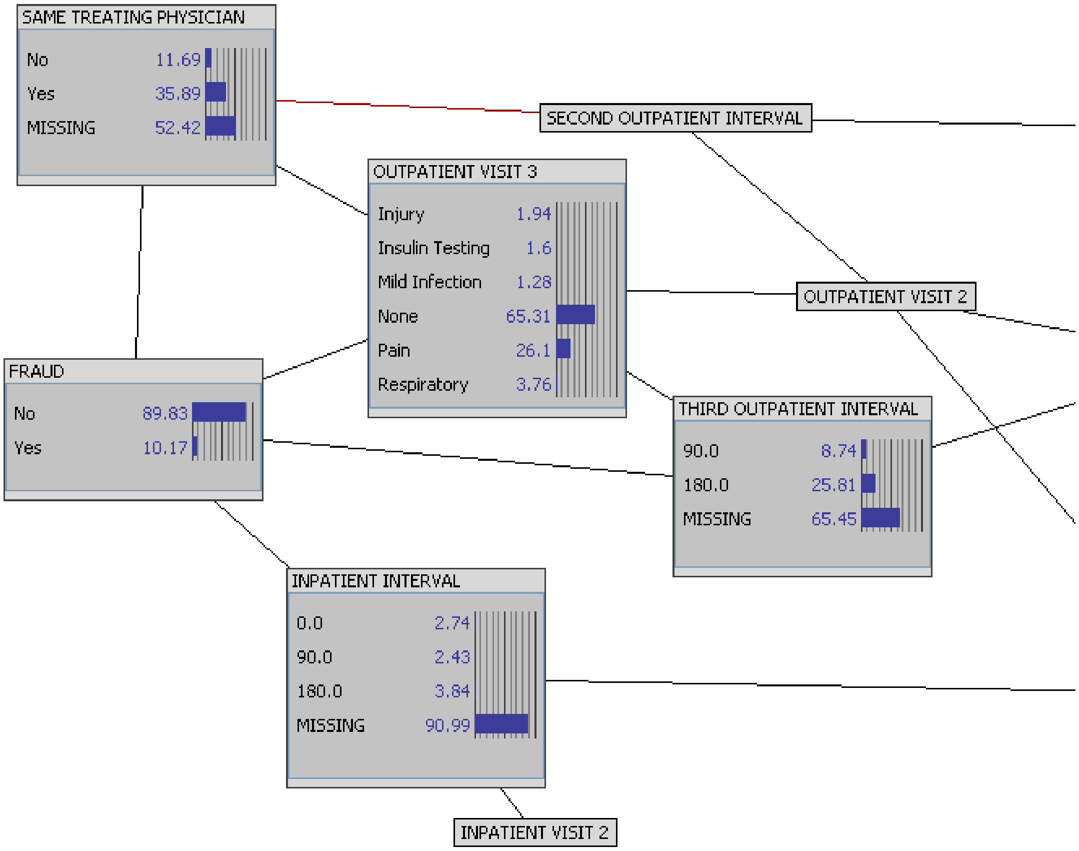


Figure 3

Evidence Input: Changed Physician

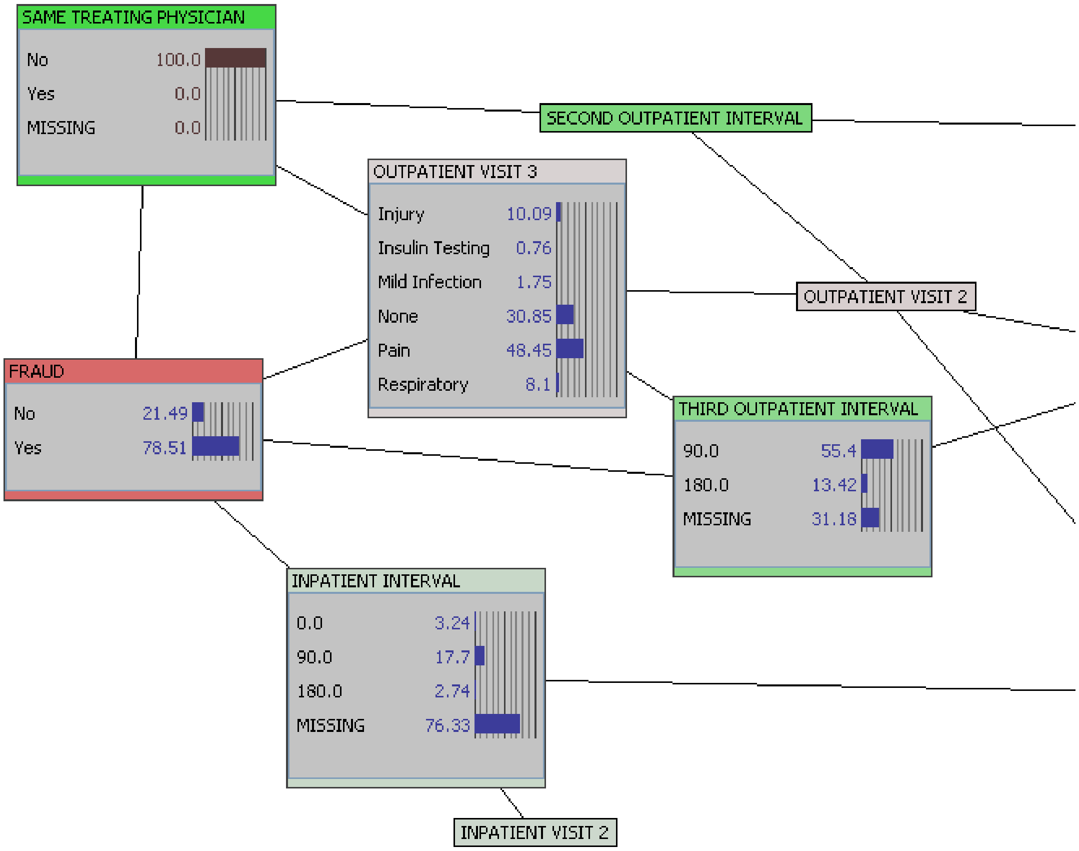


Figure 4

Evidence Input: Committed Fraud

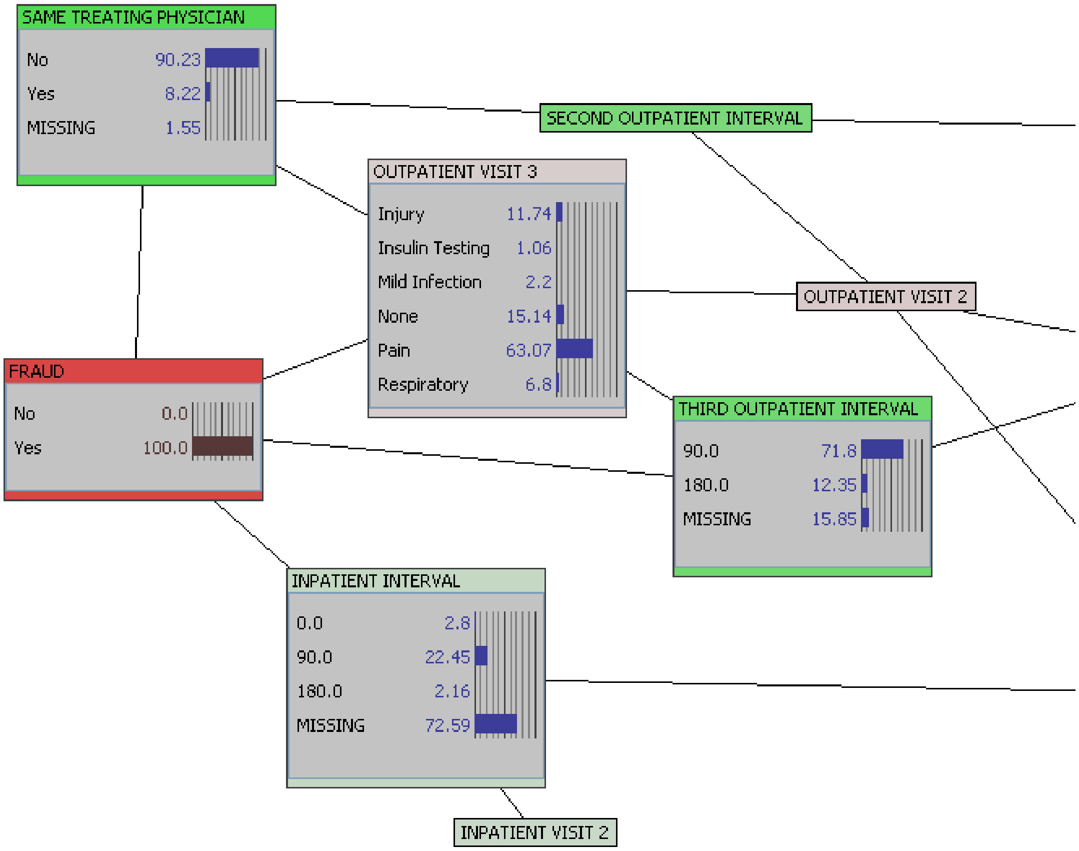


Figure 5

Probability of Fraud with Change in Physician But Limited Encounters

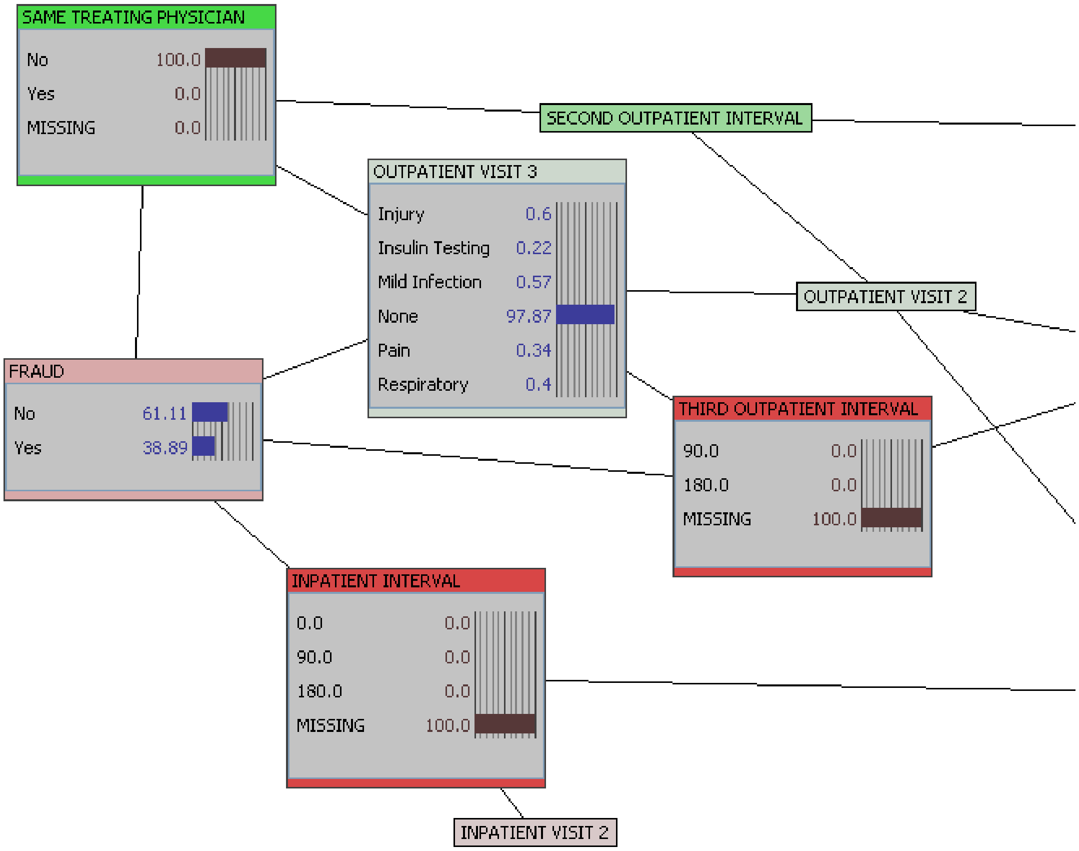
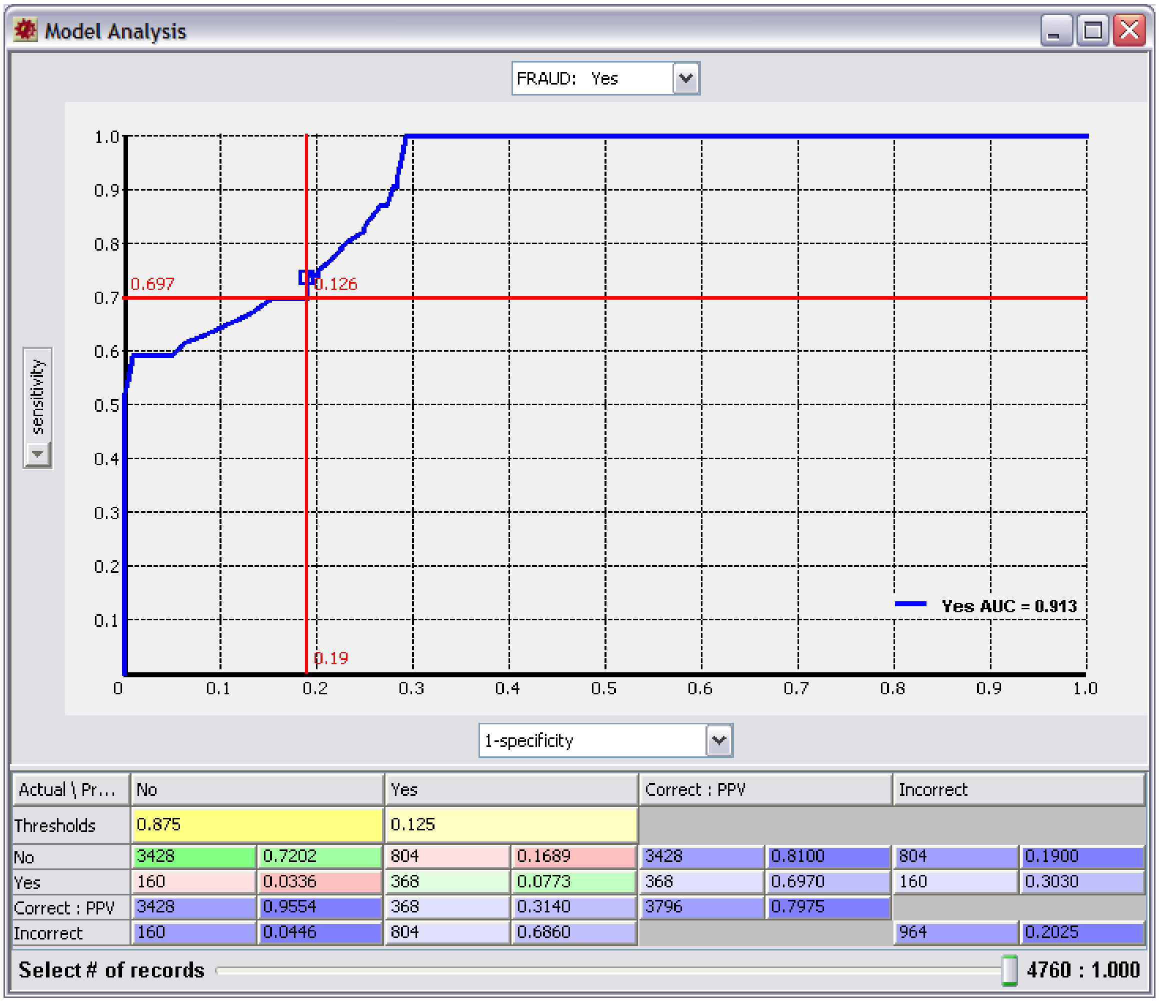


Figure 6

Receiver Operating Characteristic Curve Optimized toward Sensitivity

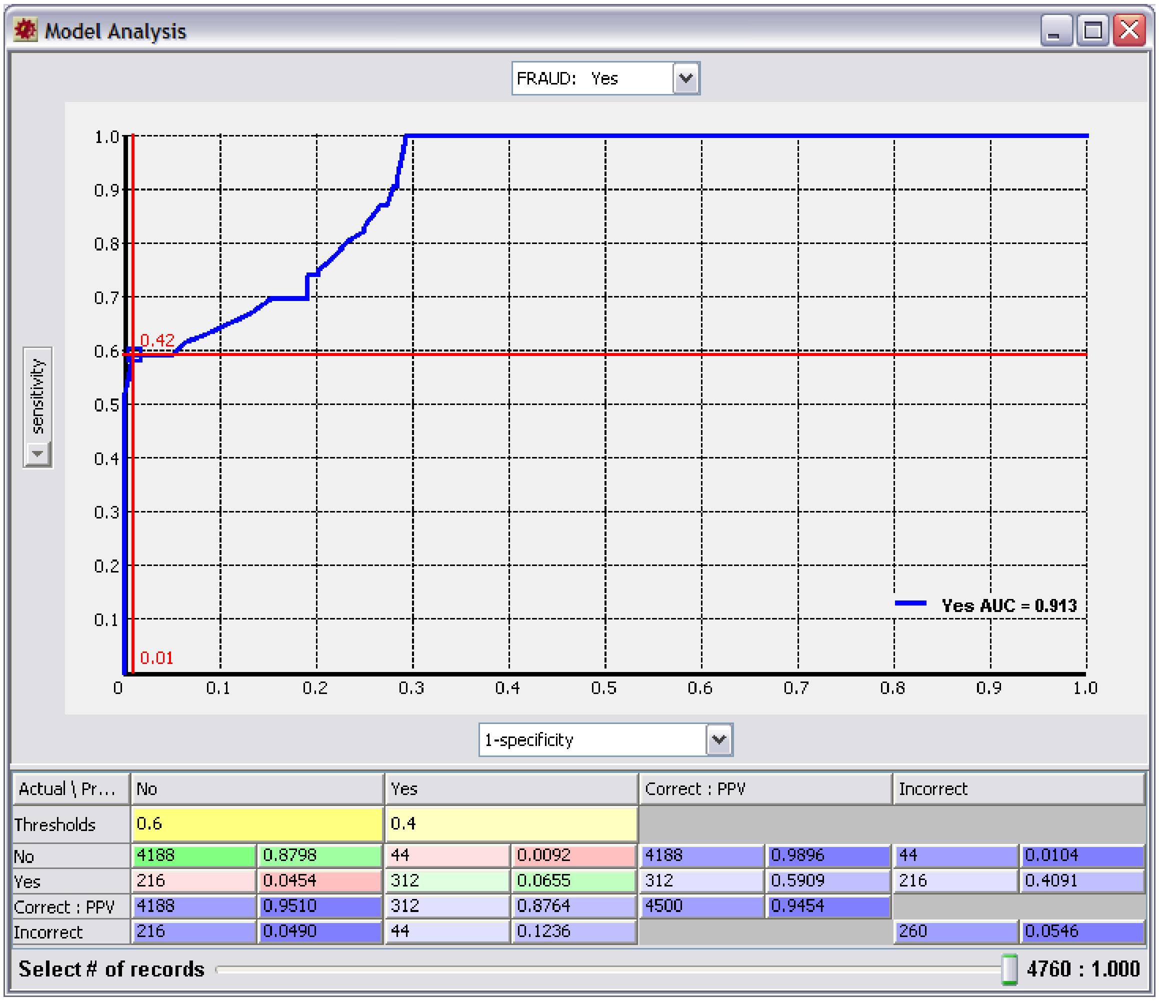


Actual \ Pr...	No		Yes		Correct : PPV		Incorrect	
Thresholds	0.875		0.125					
No	3428	0.7202	804	0.1689	3428	0.8100	804	0.1900
Yes	160	0.0336	368	0.0773	368	0.6970	160	0.3030
Correct : PPV	3428	0.9554	368	0.3140	3796	0.7975		
Incorrect	160	0.0446	804	0.6860			964	0.2025

Select # of records 4760 : 1.000

Figure 7

Receiver Operating Characteristic Curve Optimized toward Specificity



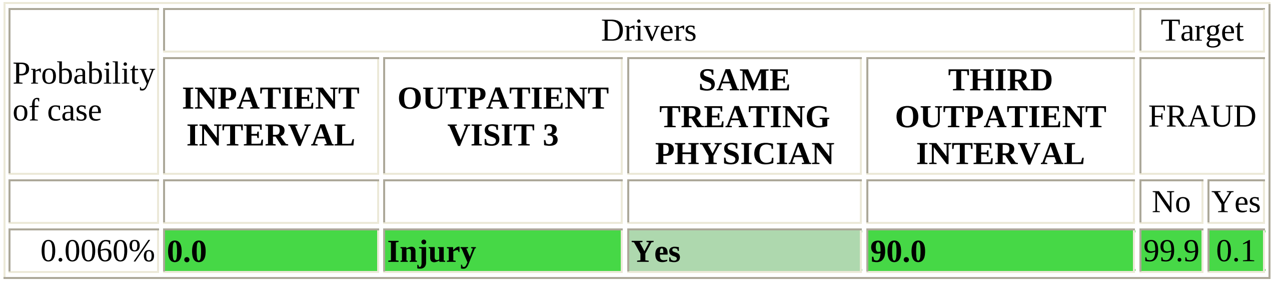
FRAUD: Yes

Actual \ Pr...	No		Yes		Correct : PPV		Incorrect	
Thresholds	0.6		0.4					
No	4188	0.8798	44	0.0092	4188	0.9896	44	0.0104
Yes	216	0.0454	312	0.0655	312	0.5909	216	0.4091
Correct : PPV	4188	0.9510	312	0.8764	4500	0.9454		
Incorrect	216	0.0490	44	0.1236			260	0.0546

Select # of records 4760 : 1.000

Table 1

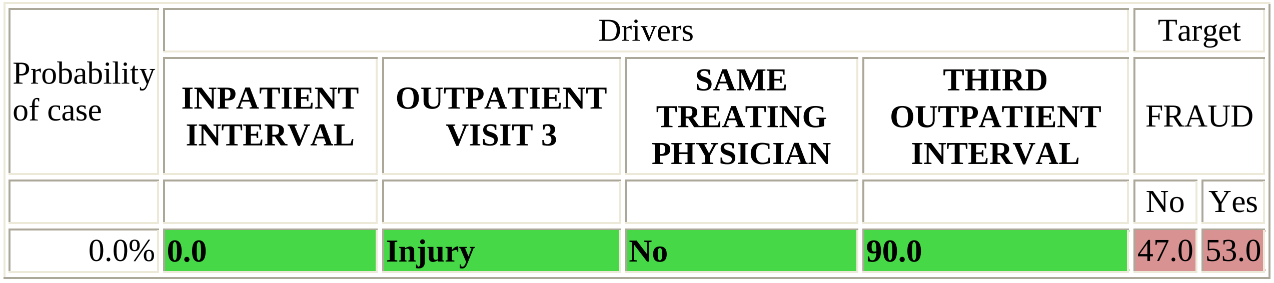
Injured Patient with Short Interval and Same Physician



Probability of case	Drivers				Target	
	INPATIENT INTERVAL	**OUTPATIENT VISIT 3**	**SAME TREATING PHYSICIAN**	**THIRD OUTPATIENT INTERVAL**	FRAUD	
					No	Yes
0.0060%	**0.0**	**Injury**	**Yes**	**90.0**	99.9	0.1

Table 2

Injured Patient with Short Interval and Different Physician



Probability of case	Drivers				Target	
	INPATIENT INTERVAL	**OUTPATIENT VISIT 3**	**SAME TREATING PHYSICIAN**	**THIRD OUTPATIENT INTERVAL**	FRAUD	
					No	Yes
0.0%	**0.0**	**Injury**	**No**	**90.0**	47.0	53.0

Table 3

Injured Patient with Different Physician, Short Outpatient Interval, and Long Inpatient Interval

Probability of case	Drivers				Target	
	INPATIENT INTERVAL	**OUTPATIENT VISIT 3**	**SAME TREATING PHYSICIAN**	**THIRD OUTPATIENT INTERVAL**	FRAUD	
					No	Yes
0.0010%	**180.0**	**Injury**	**No**	**90.0**	78.8	21.2