A STUDY OF HEALTH CARE FRAUD AND ABUSE: IMPLICATIONS FOR PROFESSIONALS MANAGING HEALTH INFORMATION

Submitted
to
3M Health Systems, Inc

by

AHIMA Foundation

This research was made possible through unrestricted funding from

3M Health Systems, Inc.

November 4, 2010

Executive Summary

Health care fraud and abuse is not only an economic drain on our health care system, but costs our nation in terms of the health of our citizens. Although significant attention has been paid to health care fraud and abuse, it is estimated that only between 3%-10% of fraud and abuse is identified. This paper examines various characteristics associated with different types of fraud and abuse, and examines the important role of the health information professional in helping to mitigate fraud and abuse.(1-6) Data were abstracted from the Health and Human Services (HHS), the Department of Justice (DOJ) and the National Health Care Anti-Fraud Association (NHCAA) annual reports for FY 2005-2007 (N=145). Using Bayesian modeling, findings of this report indicate that direct care providers (typically providers practicing in small office settings) are more likely to commit financial and misbranding types of fraud, be convicted of criminal rather than civil offenses, and receive longer jail sentences, compared to large corporate or company officials.

As our health care system shifts into an electronic environment, the health information management (HIM) professional is in a key position to help identify and mitigate health care fraud and abuse. Increasing audit oversight and more stringent enforcement creates the need for additional HIM professionals. The ONC recently offered fourteen suggestions on ways the HIM professional may be involved in fraud detection ranging from provider identification to documentation to patient identity proofing (18). For example, some of the most common types of fraud are financial fraud which includes unlawful billing and false claims - all of which are tied into aspects of the health care organization within the purview of the health information manager.

The HIM professionals are in a position to exert greater leadership in their respective provider organizations and at a national level in three specific areas:

1) *Provision of education (compliance/privacy and security guidelines, data management software technologies, and patient education (e.g., personal health records, identity theft).*

   The HIM field must continue to emphasize continuing education on new regulations and laws pertaining to fraud and abuse. Standardized refresher courses on compliance, privacy and security, HIPAA, and coding need to be emphasized and offered to all members.

2) *Proficiency on the use of Computer Assisted Coding (CAC) technologies and statistical algorithms.*

   Fraud and abuse is likely to occur over a several year time frame, therefore, CAC software can be used to create more accurate and detailed audit trails that will improve pre-pay and post-payment audits to detect coding errors and fraudulent practices over time.

   Additional HIM training efforts are needed in new electronic health record (EHR) and personal health record (PHR) technologies related to data capture, monitoring, mining, analysis, and reporting.

3) *Participation in leadership roles on both provider organization and national compliance and fraud and abuse committees and initiatives.*

   Being not only the “keepers of the record” but being involved in coding, transcription, compliance, privacy, and health information technology (HIT) strategically places HIM professionals in every critical area that is evolving in

the health care system. This charge to keep the record accurate and the move to an electronic record have opened the door to the future for the HIM professional. No longer just a steward of a paper record, by training themselves in every aspect of hospital administration from coding and cash flow, to information systems and security, the HIM professional has become a technically savvy liaison and advocate between users and information systems specialists. If HIM professionals continue to embrace these new challenges, develop new and better skill sets and adopt high professional standards, their contributions to health care savings and reform will be widely valued and recognized.

Active involvement in auditing and enforcement and the Centers for Medicare & Medicaid Services (CMS) expanded fraud and abuse detection activities will heighten awareness of the HIM professionals' increasing role within the health care arena. It will foster a need for additional research on the impact of HIM professionals in the recognition and prevention of health care fraud and abuse.

Several recommendations are proposed:

1) More HIM professionals need to be actively involved (in policy decisions) at the national and local level related to fraud and abuse prevention and detection.
2) The HIM field must continue to emphasize continuing education on new regulations and laws pertaining to fraud and abuse.
3) More research is needed on the impact of HIM professionals in the recognition and prevention of health care fraud and abuse.

Recommendations that require additional funding and legislation are also proposed:

1) Increase the number of trained HIM professionals to take the lead in medical record review and development of algorithms to detect coding and financial fraud and abuse.
2) Fund research to develop validated screening tools that are more sensitive and can be applied at a general level in detecting patterns of fraud and abuse in a proactive manner.

HIM professionals are often on the front line of the health care system and are in a position to detect fraudulent activities. Acknowledging and accepting our professional responsibility as stewards of the health care record might be the most valuable asset in combating our nation's fraud and abuse**.** As leaders in the area of the personal health record (PHR), we must become more visible as well as increase our efforts to inform the consumers of health care about potential personal issues of fraud and abuse, especially medical identity theft and privacy and security. The identification of fraud and abuse is the responsibility of all health care stakeholders including provider organizations, manufacturers, and patients.

ABSTRACT

Health care fraud and abuse is not only an economic drain on our health care system, but costs our nation in terms of the health of our citizens. Although significant attention has been paid to health care fraud and abuse, it is estimated that only 3%-10% of fraud and abuse is identified. This paper examines various characteristics associated with different types of fraud and abuse, and examines the important role of the health information professional in helping to mitigate fraud and abuse. Data were abstracted from the Health and Human Services (HHS), the Department of Justice (DOJ) and the National Health Care Anti-Fraud Association annual reports for FY 2005-2007 (N=145). Using Bayesian modeling, findings of this report found that direct care providers and provider offices are more likely to commit financial and misbranding types of fraud, be convicted of criminal rather than civil offenses, and receive longer jail sentences than large corporate or company officials. It is suggested that the HIM professional is in a key role to help identify and mitigate health care fraud and abuse. As our health care system shifts into an electronic era in terms of both the medical record and data collection, within the electronic environment, there are three specific areas where the HIM professionals can exert greater leadership both in their respective provider organizations and at a national level: 1) Provision of education (compliance/privacy and security guidelines, data management software technologies, and patient education (e.g., personal health records, identity theft); 2) Proficiency on the use of Computer Assisted Coding (CAC) technologies; and 3) Increased visibility and leadership roles on both provider organization and national compliance and fraud and abuse committees and initiatives.

Introduction

Few, if any, health care professions combine the expertise of health information management (HIM) professionals in the legal aspects of the Electronic Health Record, Health Information Exchange (HIE), compliance with regulatory policies and guidelines, coding, billing, and data management. As the federal government recommits itself to fight fraud and abuse, the role of the health information professional will become increasingly important. As noted in his address to a joint session of Congress, February 24th 2009, President Obama promised to "root out the waste, fraud, and abuse in our Medicare program that doesn't make our seniors healthier".(1) To back this commitment, the Obama administration allocated a $1.7 billion increase over 5 years to support the Health Care Fraud and Abuse Control (HCFAC) program in the FY 2010 budget. In addition to the increased financial support, on May 20th 2009, Department of Justice (DOJ) Attorney General Holder and Health and Human Services (HHS) Secretary Sebelius announced the creation of an interagency effort, the Healthcare Fraud Prevention and Enforcement Action Team (HEAT), a combined effort of the DOJ and HHS to further address issues of fraud and abuse. The role of the HEAT team was expanded to include:(2)

- Increased site visits to potential suppliers,
- Increased training on Medicare compliance for health care providers,
- Improved data sharing between CMS and law enforcement, and
- Increased monitoring of Medicaid Parts C (Medicare Advantage (MA)), and D (the Medicare Prescription Drug Benefit)

The seriousness of the government's efforts to prosecute offenders can be seen in several landmark cases ranging from prosecuting small health care providers such as Mercy Medical Center in Sioux City, Iowa to large corporations such as Pfizer. In December 2009, Mercy Medical Center "agreed to pay the United States $400,000 to settle allegations it violated the False Claims Act by inflating charges for heart patients' care".(3) On September 3, 2009, officials from DOJ and HHS announced a $2.3 billion settlement with the Pfizer Unit Pharmacia & Upjohn.(4) Pfizer pleaded guilty to one felony count of illegal marketing of Bextra (an anti-inflammatory drug) for extended usage and higher doses than approved by the Federal Drug Administration (FDA).(4) These types of landmark cases have signaled the Obama administration's increased effort to highlight fraud and abuse as the centerpiece to this administration's health care reform.

To better understand the nature and process of health care fraud and abuse in the context of health information management, this paper will provide an initial pilot test of a predictive Bayesian statistical model that examines successfully prosecuted Federal cases of fraud and abuse. Data for this paper were collected from the HCFAC annual reports for 2006-08 (FY 2005-07). All fraud and abuse cases outlined or reported in the HCFAC annual reports were included in the analysis (N=145).

Significance

According to the Office of Management and Budget's fact sheet "*Transforming and Modernizing America's Health Care",* the United States spends roughly $8,000 per person or $2.2 trillion per year on health care. This figure is expected to rise to approximately $4 trillion by 2017.(2, 6,7) Conservative estimates of the cost of fraud and

abuse within our health care system range from 3%-10% or between $66 billion and $220 billion per year. With the expected increase in the cost of health care, the cost of health care fraud and abuse could easily rise above $400 billion per year by the year 2017.(2,7) Health care fraud and abuse is not only an economic drain on our health care system, but costs our nation in terms of the health of our citizens (Semi-Annual Report to Congress October 1 2008-March 31-2009 (2): Office of the Inspector General (1)).

Fraud and abuse schemes often place patients in situations of unnecessary risk of injury or even death.(6) Patients may be exposed to over medication (as in the Pfizer case of Bextra), or even subjected to unnecessary surgeries.(6) For example, in 2002 a cardiologist in Chicago was charged with performing over 750 unnecessary catheterizations over a 10 year period of time.(2)

Fraud and abuse not only costs our nation in terms of health care dollars and patient care, but it is also against the law. Under the Health Insurance Portability and Accountability Act 1996 (HIPAA) (18USC, CH.63, Sec.1347), “fraud is defined as knowingly, and willfully executes or attempts to execute a scheme … to defraud any health care benefit program or to obtain by means of false or fraudulent pretenses, representations, or promises any of the money or property owned by …. any health care benefit program…”. Health care abuse is defined in terms of “practitioner practices that are inconsistent with accepted sound fiscal business or medical practices which directly or indirectly may result in: 1) unnecessary costs to the program, 2) improper payment, 3) services that fail to meet professionally recognized standards of care or are medically unnecessary, or 4) services that directly or indirectly result in adverse patient outcomes

or delays in appropriate diagnosis or treatment."(Federal Register pg 58345 1998 http://www.npdb-hipdb.hrsa.gov/legislation/fedreg/Federal_Register_1998-10-30.pdf)

The Bayesian analysis will examine how the type of fraud is linked to penalties, type and size of provider, and region of the country.

Methodology

Data for the study were collected from the HCFAC annual reports 2006 (n=32), 2007 (n=58), and 2008 (n=55), for fiscal years 2005-2007. All fraud and abuse cases outlined in the HCFAC annual reports were included in the analysis (N=145).

Variables

Data from the HCFAC annual reports were abstracted by two independent coders in a two step process and then compared for accuracy at each step. One coder was an exercise science student interested in attending medical school, the other coder (supervisor) was an experienced data analyst and Registered Health Information Administrator (RHIA). When discrepancies existed in abstraction or coding processes, either authors of this paper or a senior research analyst resolved the discrepancy. In step 1, coders abstracted codes from the text of the report (92% agreement). In step 2, coders assigned numerical codes to the abstracted data to be used in the Bayesian models (84% agreement). From this process, the following 8 variables were abstracted and used in the data analysis:

1. **Who was Charged with the Fraud**: 1. Direct Care Provider (e.g., physician, nurse, physical therapist), 2. Company Officials (e.g., CEO, CFO)
2. **Type of Business**: 1. Direct Retail (e.g., physician office), 2. Manufacture (e.g., drug company)

3. **Penalty**: 1. Civil, 2. Criminal, 3. Civil and Criminal

4. **Financial Penalty (**in Millions**)**

5. **Penalty in Jail Time** (months)

6. **Length of Fraud** (months)

7. **Region of the Country**: 1. East, 2. Midwest, 3. South, 4. West, 5. Involved Foreign Country, and 6. Unknown

8. **Type of Fraud**

   a. False Claims and Statements

   b. Financial Fraud (embezzling, money laundering, unlawfully billing)

   c. Illegal Practice of Medicine (unlicensed physicians, violation of physician self referral act)

   d. Illegal kickbacks (receiving and paying)

   e. Mail Fraud

   f. Misbranding (misbranding of drugs, illegal marketing, illegal distribution and selling, use of unapproved drugs, use of counterfeit drugs)

   g. Prescribing (forged signatures and documents)

   h. Coding

Table 1 provides examples of each type of fraud. For purposes of the statistical modeling, where more than one type of fraud is mentioned, we divided the type of fraud and abuse into 3 separate variables reflecting the number of types of fraud and abuse per case (one type of fraud/case, two types of fraud/case, and three types of fraud/case.

However, only 7 of the cases reflected three types of fraud/case, consequently, this variable was left out of the analysis.

Bayesian Model

Data for this study were analyzed using machine learning Bayesian Modeling software. Bayesian networks encode the information structure of the problem using conditional dependence relationships between variables (e.g., the statistical likelihood of an outcome given the presence or absence of other factors). The structure of the network provides the user with immediate knowledge about the nature of the problem set and the relative significance of variables to the outcome of interest. By entering current knowledge into the model, the user obtains a probability of outcome, and relative risk in real time. Further, the graphical representation of the network also provides the user with likely rationale for the outcome and knowledge about additional information required to confirm or refute the predicted outcome. Relationships in the Bayesian analysis are based odds ratios, not correlations.

Data Analysis

Frequency Analysis

Data reporting the frequencies for *who* was charged with fraud, *type of business*, *penalty*, and *region* of the country are reported in Table 2.

Data from Table 2 show that:

- 69.7% of the cases prosecuted and convicted were *companies* and 30.3% were *direct care providers*

- 45.9% resulted in civil convictions, 43.2% criminal convictions, and 6.2% criminal and civil convictions.

The number and percentage for each type of fraud is depicted in Table 3.

- In terms of the types of fraud, financial fraud (embezzling, money laundering, unlawfully billing) and false claims statements were the most common (48.9% and 32.4%, respectively).
- Coding and mail fraud were the least common types of fraud prosecuted and convicted at 2.1%.

Results from Bayesian Analysis

Findings from the Bayesian analysis are provided in Figure 1. Findings from this model show that: *Who is charged*, and the *Type of business* are the two key variables central to the model. *Who is charged* (Direct care provider or the Company) is directly related to length of fraud in months, penalty in jail, whether the charge is civil or criminal, the dollar amount of the fine and most importantly, the type of fraud. Similarly, whether the entity committing the fraud is a manufacturer (e.g., Pfizer) or direct retail (e.g., physician office or hospital) is directly related to whether it is a civil or criminal charge, penalty of the fine, region of the country, and type of fraud.

Figure 2 provides data on only direct care providers and direct care retailers; while, Figure 3 provides information only on manufacturing companies and company executives (e.g., CEO, CIO) prosecuted and convicted of fraud and abuse. When we compare data from these two figures, we find that the nature of the fraud and abuse and

penalties are very different. For example, direct care provider and direct retailers are very different than manufacturers and company executives in the type of fraud, type of penalty (civil or criminal), the amount of the fine and amount of jail time. Direct care providers who work in hospitals or physician offices are much more likely to be convicted of financial fraud, 47% to 17%, (embezzling, money laundering, unlawfully billing); while, manufacturing companies and company executives are more likely to be convicted of misbranding, 50% to 24%, (misbranding of drugs, illegal marketing, illegal distribution and selling, use of unapproved drugs, use of counterfeit drugs). Direct care providers and retailers are more likely to be convicted of criminal charges (79% to 11%) and spend time in jail (76% to 17%). Manufacturing companies and company executives are more likely to be convicted of civil charges (74% to 9%) and receive much higher fines (>$22 million 70% to 6%).

While we do not have direct data to support an explanation, there is anecdotal data suggesting that some of the differences are related to having a “culture of compliance”. Small practices generally do not have a compliance plan in place and do not have the resources to hire sophisticated legal counsel trained specifically on health care fraud and abuse. Fraud and abuse is seen as being blatant and directly related to care issues. On the other hand, large organizations generally have a compliance plan in place (based on the federal sentencing guidelines) and have legal counsel specifically trained in health care fraud and abuse. As such, the “compliance plan” serves as a mitigating factor in whether or not jail time is imposed. Consequently, the fraud and abuse is seen as a systemic failure not tied directly to one individual.

Discussion: Implication for Health Information Managers

As the role of the health information manager expands to meet demands of the electronic health information network, so is the need for health information managers to help in the mitigation of fraud and abuse. As health information professionals, we need to step beyond the traditional role of focusing only on coding and to embrace our broader role within the HIT/HIM environment.(7) Data abstracted from the HCFAC annual report, and noted in this study, found the most common types of fraud are financial fraud which includes unlawfully billing and false claims - all of which are tied to aspects of the health care organization related patient identification and data security.

Within the electronic environment, there are three specific areas where the HIM professionals can exert greater leadership both in their respective provider organizations and at a national level:

1. Education
   a. Compliance/privacy and security guidelines
   b. Data management software technologies
   c. Patient education (e.g., personal health records, identity theft)
2. Proficiency on the use of Computer Assisted Coding (CAC**)** technologies and new CMS coding algorithms
3. Increase visibility and leadership roles in both provider organization and national compliance and fraud and abuse committees and initiatives

Education

First, the HIM field must continue to emphasize continuing education on new regulations and laws pertaining to fraud and abuse. Standardized refresher courses on

compliance, privacy and security, HIPAA, and coding need to be emphasized and offered for all members. As a profession we must make sure that all staff have been properly trained and receive ongoing continuing education. We need to continue to expand our role within the health care environment as the 'go to' experts in issues related to fraud and abuse.(8-17)

Second, we need to increase our training efforts on new electronic health record (EHR) technologies related to data capture, monitoring, mining, analysis, and reporting.(18, 19) A recent report by the ONC (18) offered the following fourteen suggestions as to how the EHR would provide better data for the HIM professional by increasing data accuracy and aid in fraud management:

1. Audit functions and features
2. Provider identification
3. User access authorization
4. Documentation
5. Evaluation & Management (E&M) Coding
6. Proxy authorship
7. Record modification after signature
8. Auditor access to patient records
9. EHR traceability
10. Patient involvement
11. Patient identity-proofing
12. Structured and coded data
13. Integrity of EHR transmission

14. Accurate linkage of claims to clinical records.

Third, we must remember that fraud and abuse is the responsibility of all health care stakeholders including provider organizations, manufacturers, and patients. As leaders in the area of the personal health record (PHR), we must become more visible as well as increase our efforts to inform the consumers of health care about potential personal issues of fraud and abuse (e.g., medical identity theft and privacy and security).

Computer Assisted Coding (CAC) Technologies

Several articles have documented the importance of CAC technology in helping to deal with fraud and abuse.(19-25) CAC software provides the HIM professional with real time prompts and decision support tools. This in turn should help to reduce fraudulent claim submissions by providing information for the accurate and timely documentation required for specified levels of care. Increased monitoring of compliance with identified standards and protocols should help to reduce fraud and abuse and create a system of integrity. As reported in our findings section, fraud and abuse is likely to occur over a several year time frame, therefore, CAC software can be used to create more accurate and detailed audit trails that will improve pre-pay and post-payment audits to detect coding errors and fraudulent practices over time.

Increased Participation and Leadership on Provider and National Compliance and Fraud and Abuse Committees and Initiatives

HIM professionals are often on the front line of the health care system and are in a position to detect fraudulent activities. Acknowledging and accepting our professional responsibility as stewards of the health care record might be the most valuable asset in

combating our nation's fraud and abuse**.** Furthermore, the HIM profession has distinguished itself as the leader in the development of the PHR. Within the provider network it is essential that the HIM professional plays an integral role on committees that develop comprehensive internal policies and procedures for coding and billing in order to ensure that written procedures are accurate and kept up-to-date and that the HIM professionals communicate their extensive knowledge to senior leaders within their organizations.

As noted earlier, controlling fraud and abuse is at the forefront of health care reform. Given the educational and skill sets that HIM professionals have developed with regard to data management, privacy and security/legal training, and involvement in HIT implementation, it is important that the HIM profession becomes increasingly involved in regulatory policies and procedures related to fraud and abuse. The HIM profession should be brought in as the external experts that will provide unbiased evaluation in the development and implementation of guidelines and processes related to detecting fraud and abuse. The HIM profession has the potential to contribute not only in terms of policy and procedural issues, but also in developing educational programs for both the patient (e.g., PHR) and the providers.

Implications for Policy Makers

Current national policy toward fraud and abuse seems to be based more on a reactive penalties and prosecution rather than proactive development of legislative actions to stop fraud and abuse. Findings from this research, along with prior research, would suggest that taking a more proactive approach to prevent fraud and abuse may

prove to be more beneficial. This would suggest a three-pronged approach in providing legislation and funding that would:

1) Increase the number of trained HIM professionals to take the lead in record review and development of algorithms to detect coding and financial fraud and abuse;
2) Develop validated screening tools that are more sensitive and can be applied at a general level in detecting patterns of fraud and abuse in a proactive manner; and
3) Seek participation of HIM leaders in national compliance and fraud and abuse committees and initiatives.

Conclusions

How does health care fraud impact HIM? HIM professionals are often on the front line of the health care system and are in a position to potentially detect fraudulent activities. Acknowledging and accepting our professional responsibility as stewards of the health care record might be the most valuable asset in combating fraud and abuse in the nation's health care system. As the traditional "keepers of the record" we are entrusted with the accurate translation and documentation of each patient incidence of care. It is this record that is the basis for all treatment and reimbursement. Being not only the "keepers of the record" but being involved in coding, transcription, compliance, privacy, and HIT places HIM professionals strategically in every critical area that is evolving in the health care system. This charge to keep the record accurate and the move to an electronic record have opened the door to the future for the HIM professional. No longer just a steward of a paper record, by training themselves in every

aspect of hospital administration from coding and cash flow, to information systems and security, the HIM professional has become a technically savvy liaison and advocate between users and information systems specialists. If HIM professionals continue to embrace these new challenges, develop new and better skill sets, and adopt high professional standards, their contributions to health care savings and reform will be widely valued and recognized.

Recommendations

Several recommendations are suggested:

1) HIM professionals need to be involved actively in policy decisions at the national and local level related to fraud and abuse prevention and detection.
2) HIM professionals need to be actively involved with national and local organizations fighting fraud and abuse.
3) More research is needed on the impact of HIM professionals in the recognition and prevention of health care fraud and abuse.

TABLES AND FIGURES

Table 1. Examples of the Types of Fraud False Claims and Statements

False Claims and Statements	A physician office submits false claims to Medicare for medically unnecessary durable medical equipment (DME)
Financial Fraud	A company bills Medicare more than was necessary for medical services
Illegal Practice of Medicine	An physician, unlicensed to practice, sees patients and bills for services
Illegal Kickbacks	A manufacturer pays doctors a bogus consulting fee to induce them to purchase its product
Mail Fraud	A health care attorney prepares false documents in an attempt to gain approval for a joint venture agreement between a physician group and a physical therapy company
Misbranding	A pharmaceutical company misbrands a drug's properties
Prescribing Fraud	A physician prescribes controlled substances that are not medically necessary
Coding	A physician group up-codes for medical services

Table 2. Frequencies for the variables: Who was charged with the Fraud and Abuse? What Type of Business? What was the Legal Penalty? What Region of the Country?

Variable	Variable Names	Number of Cases	Percent
Who was Charged?	1. Company 2. Direct Care Provider	1. 101 2. 44	1. 69.7% 2. 30.3%
Type of Business	1. Manufacture 2. Direct Retail	1. 17 2. 128	1. 11.7% 2. 88.3%
Legal Penalty	1. Civil 2. Criminal 3. Civil and Criminal (Missing)	1. 67 2. 63 3. 9 4. 6	1. 45.9% 2. 43.2% 3. 6.2% 4. 4.8%
Region of the Country	1. East 2. Mid-West 3. South 4. West 5. Foreign Country (Missing)	1. 29 2. 35 3. 49 4. 22 5. 2 6. 9	1. 19.9% 2. 24.0% 3. 33.6% 4. 15.1% 5. 1.4% 6. 6.2%

Table 3. Frequencies and Percentages for the Type of Fraud*

Type of Fraud	Frequency	Valid Percent
Misbranding	25	17.2%
Financial Fraud	71	48.9%
Illegeal Kickbacks	21	14.5%
False Claims & Statements	47	32.4%
Illegal Practices	8	5.5%
Prescribing Fraud	8	5.5%
Mail Fraud	3	2.1%
Coding	3	2.1%

*** Frequencies and Percentages exceed the N=145 since multiple choices for Type of Fraud are documented in the reports.**

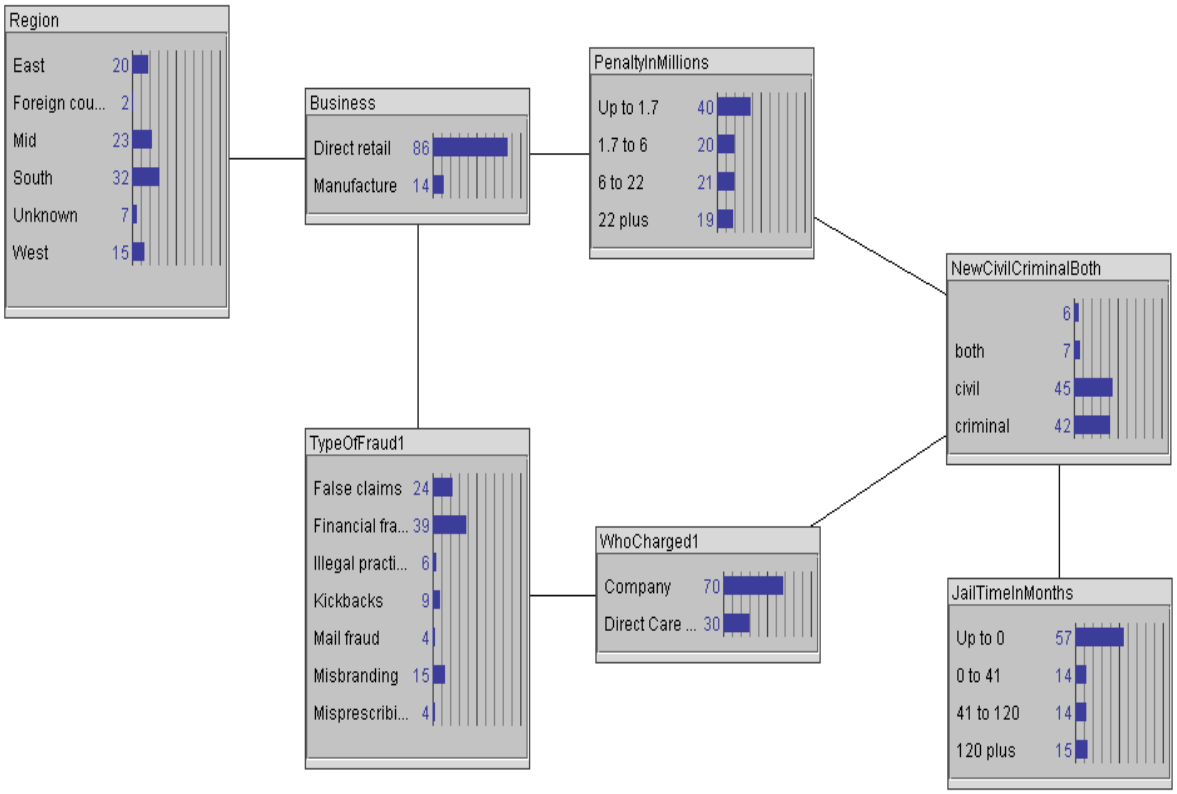

Figure 1. Bayesian Belief Network of Factors Related to Fraud and Abuse

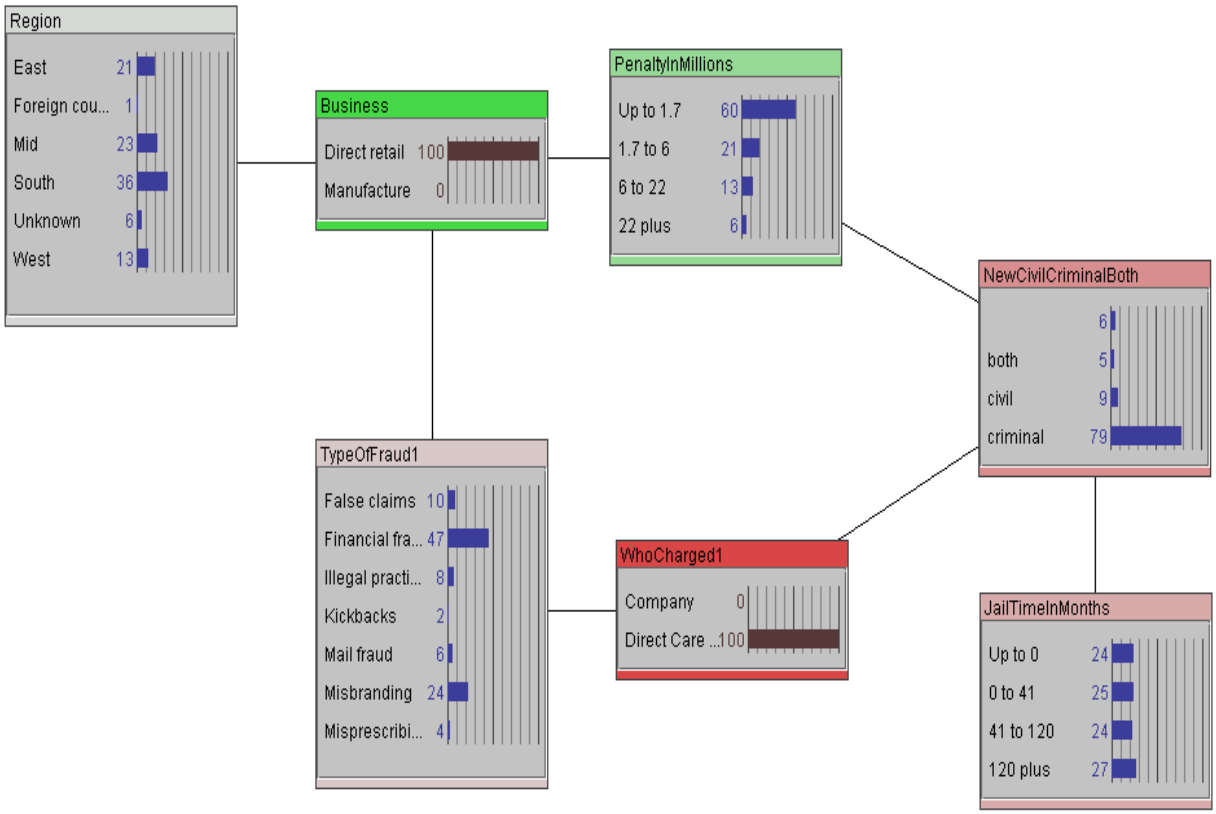

Figure 2. Bayesian Belief Network of Factors Related to Fraud and Abuse holding constant Who was charged (Direct care provider) and Type of Business Charged (Direct retailer).

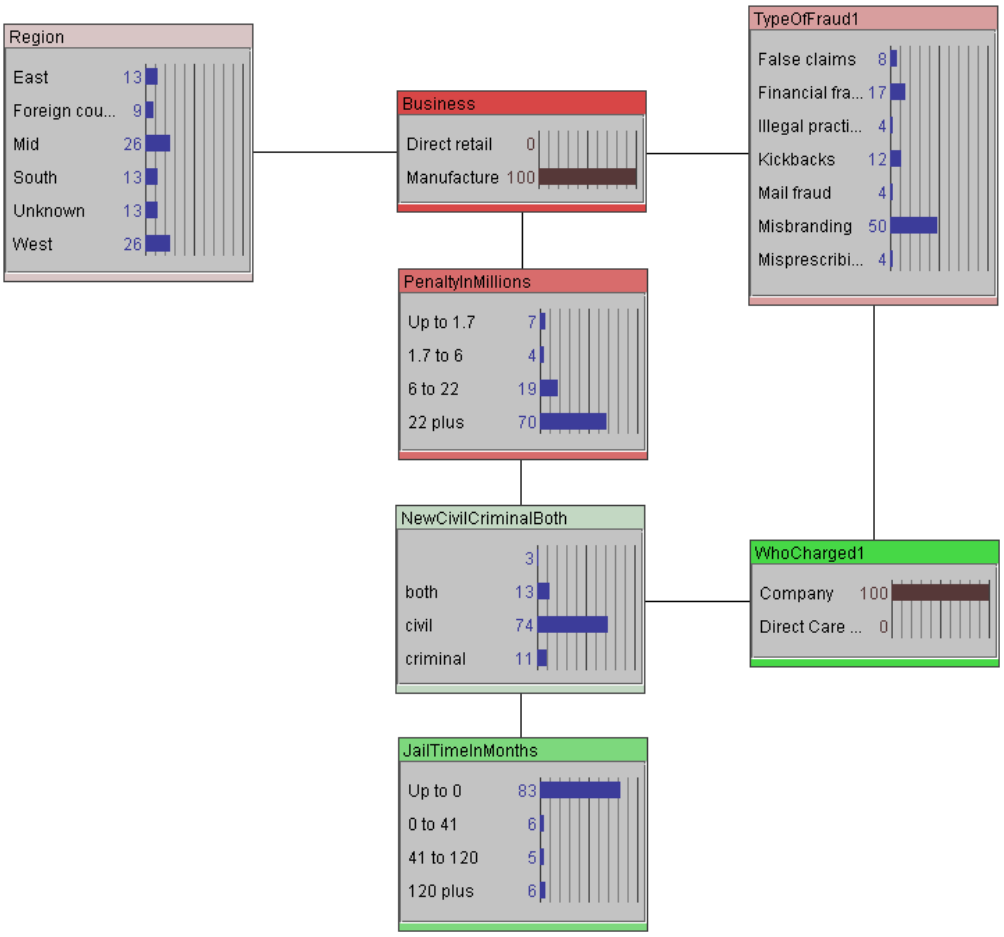

Figure 3. Bayesian Belief Network of Factors Related to Fraud and Abuse holding constant Who was charged (company executives) and Type of Business Charged (manufacture).

References

1. http://www.reobama.com/SpeechesFeb2409.htm
2. Semi-Annual Report to Congress October 1 2008-March 31-2009, Office of the Inspector General
3. http://www.justice.gov/usao/ian/index.html
4. pubrecord.org/law/4591/**Pfizer**-pleads-guilty-felony-**billion**
5. Federal Bureau of Investigation, Financial Crimes Report to the Public, Fiscal Year 2007
6. Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Expenditure Projections 2007-2017
7. National Health Care Anti-Fraud Association report *"The Problem of Health Care Fraud. Consumer Alert: The impact of Health Care Fraud on You"* 2008
8. The Department of Health and Human Services (HHS) and Department of Justice (DOJ), Health Care Fraud and Abuse Control Program Annual Report for FY2005-2007 (Annual Report 2006-2008).
9. Allan S Brett, *New Guidelines for Coding Physicians' Services - A Step Backward,* New England Journal of Medicine, Volume 339:1705-1708, Number 23, December 3, 1998 http://content.nejm.org/cgi/content/full/339/23/1705
10. Phillips, C D, Hillman, B J, *Coding and Reimbursement Issues for the Radiologist,* Radiology, 220 (1): 7, (2001)http://radiology.rsnajnls.org/cgi/reprint/220/1/7

11. Shane, R, *Detecting and preventing health care fraud and abuse – we've only just begun,* American Journal of Health-System Pharmacy, 57(11): 1078. (2000) http://www.ajhp.org/cgi/reprint/57/11/1078
12. Malatestinic W, Braun L A, Jorgenson, J A, Eskew J, *Components of Medicare reimbursement,* Am J Health-Syst Pharm; Vol 60 Nov 1, 2003 Suppl 6 http://www.ajhp.org/cgi/reprint/60/suppl_6/S3.pdf
13. Hand, R W, *E & M Guidelines*, Chest, 1998;113;1432-1434 http://www.chestjournal.org/content/113/6/1432.full.pdf+htm
14. King, M S, Sharp, L, and Lipsky, M S, *Accuracy of CPT Evaluation and Management Coding by Family Physicians,* JABFP, 14(3): 184 (2001)
15. Chute, C G, *Clinical Classification and Terminology – Some History and Current Observations,* JAMIA; 7:298-303; (2000) http://www.jamia.org/cgi/content/abstract/7/3/298
16. Gruber N P, Shepherd H, Varner R V, *Role of a Medical Staff Coding Committee in Documentation, Coding, and Billing Compliance,* Psychiatric Services; 53 (12): 1629. (2002) http://www.psychservices.psychiatryonline.org/cgi/reprint/53/12/1629
17. Adams, D L, Norman H, and Burroughs, V J, *Addressing medical coding and billing part II: a strategy for achieving compliance. A risk management approach for reducing coding and billing errors,* J Natl Med Assoc; 94(6): 430-447, June, 2002
18. Recommended Requirements for Enhancing Data Quality in Electronic Health Records Final Report Prepared for Kathleen H. Fyffe Senior Advisor The Office

of the National Coordinator for Health Information Technology May 2007 by RTI Sojol L, Garcia B, Rodriguez J, West

19. Sokol L, Garcia B, Rodriguez J, West M, Johnson K M, and Johnson K; Using data mining to find fraud in HCFA health care claims; Top Health Inf Manage; 2001 Aug; 22(1):1-13. http://www.ncbi.nlm.nih.gov/pubmed/11680273
20. Jiang Y, Nossal M, and Resnik P; *How Does the System Know It's Right? Automated Confidence Assessment for Compliant Coding,* Perspectives in Health Information Management, CAC Proceedings, Fall 2006
21. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_032075.pdf
22. Heinze D T, Morsch M I, Sheffer R E, Jimmink M A, Jennings M A, Morris W C, and Morsch A E; *Life Code – A deployed Application for Automated Medical Coding;* AI Magazine; Volume 22 Number 2 (2001)
23. http://www.aaai.org/ojs/index.php/aimagazine/article/viewFile/1562/1461
24. Ortega P A, Figueroa C J, and Ruz, G A; *A Medical Claim Fraud/Abuse Detection System based on Data Mining: A Case Study in Chile;* http://www.mec.cf.ac.uk/~scegr2/pub/DMI5560.pdf
25. Garvin J H, Watzlaf V, and Moeini S; *Automated Coding Software: Development and Use to Enhance Anti-Fraud Activities;* AMIA 2006 Symposium Proceedings, page 927 http://www.pubmedcentral.nih.gov/picrender.fcgi?artid=1839655&blobtype=pdf