Hospitals, Contractors and Data Mining… What's Next?

The Emergence of Advanced Data-Analysis Tools

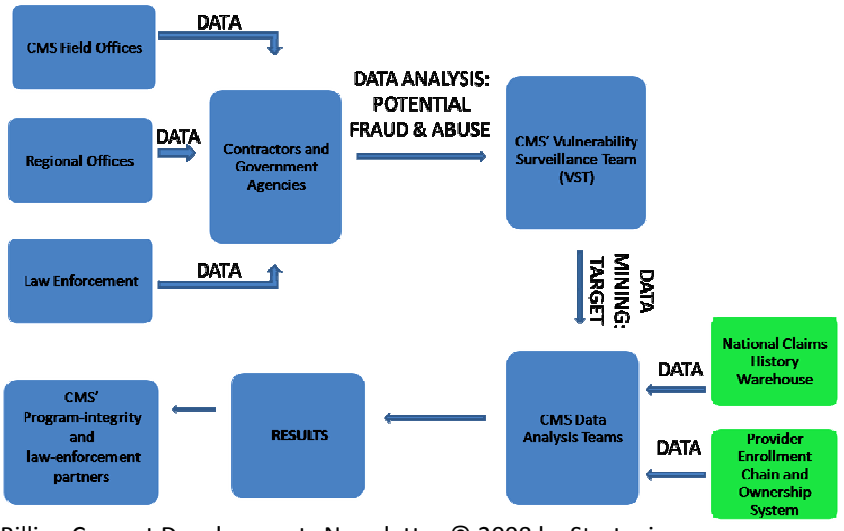
In a continual effort to decrease unnecessary medical claims as well as detect fraud and abuse against federal health care programs and beneficiaries, the Centers for Medicare and Medicaid Services (CMS) are increasingly utilizing sophisticated data analysis tools. This process, known as data mining, identifies potential payment aberrations (overpayment and underpayment) in large databases. CMS' contractors — Medicaid Integrity Contractors (MICs), Program Safeguard Contractors (PSCs), Recovery Audit Contractors (RACs), and Medicare Audit Contractors (MACs) — use data mining to identify payment aberrations, fraud and abuse in federal health care programs. Additionally, MACs are the first CMS contractors to have access to both Part A and Part B claims data. The findings that are generated from data mining are distributed to CMS' program integrity and law-enforcement partners. As a result, there is an increased likelihood for errors to be detected and hospitals to be found noncompliant with federal regulations.

Hospital management personnel, such as billers, coders, and compliance officers, are uniquely affected by data mining and need to understand how CMS intends to use the hospital's data. By obtaining insight on how the data is manipulated and assessed, hospitals will be in a position to implement similar techniques in order to identify and fix errors before CMS' contractors discover them.

The Process

Figure 1 provides an overview of how CMS detects fraud, waste and abuse. CMS has created the Vulnerability Surveillance Team (VST), which serves as the focal point for identifying improper activities in Medicare Parts A and B. The VST assesses the behavior patterns of providers and suppliers by using data mining techniques. The categories VST evaluate include but are not limited to:

Figure 1



**Atlantic Information Services is a publishing and information company that has been serving the health care industry for more than 20 years. It develops highly targeted news, data and strategic information for managers in hospitals, health plans, medical group practices, pharmaceutical companies and other health care organizations. AIS products include print and electronic newsletters, Web sites, looseleafs, books, strategic reports, databases, audioconferences and live conferences.*

- Inappropriate billing;
- Outlier payments;
- Identity theft;
- Inappropriate use of National Provider Identifiers; and
- Weak operational policies that may result in overpayments.

The VST responds to potential fraud, waste and abuse referrals provided by CMS contractors who have conducted data analyses to identify suspicious activity. With the use of data mining, the VST selects a "target" suspicious activity, i.e. increased number of home health facilities, which requires further evaluation. Subsequently, CMS' data analysis team conducts an investigation with data available in the National Claims History Warehouse and the Provider Enrollment Chain and Ownership System, which is not available for public use. The results of CMS' data analysis are used to identify anomalies. For instance, when CMS conducted a review of home health agencies between 2003 and 2006 in Miami, FL, high outlier payments for insulin shots were detected utilizing the process described above. CMS' analyses indicated that 60 shots were administered for every 120 visits. This figure was significantly higher than the national average --- 30 shots per 120 visits.

Revealing unnecessary medical expenses, fraud and abuse is not a simple task. The data analysis involved is a multistep process. Once potential suspicious activity is referred to the VST, the following steps are employed:

- **Validation.** The data must be validated to ensure accuracy. More specifically, are the reported codes correct? How accurate is the dollar amount?
- **Identification.** The improper activity and its compliant versions (e.g. policies, procedure codes, payment process, and bill types) are analyzed and discrepancies are identified.
- **Quality-control review.** A final check helps to ensure accuracy of the data analysis process.

Mimic the Process

The CMS' contractors also intend to use data mining to identify improper claims in large amounts of data. As a result, hospital management personnel are strongly encouraged to consider data mining as a part of their compliance programs and ongoing operations. For instance, the use of descriptive statistics, such as frequency, mean and standard deviation, can identify potential outliers, such as excessive use of a specific MS-DRG, upcoding, unbundling, outlier payments and billing errors. Furthermore, to predict outcomes or identify potential areas of fraud and overpayments in Medicare and Medicaid data, advanced statistical methods, such as regression modeling and clustering analyses, can be conducted.

The results obtained from statistical analyses can be compared to findings in the region or the nation. There is a substantial amount of public information available for hospitals to conduct their own comparative analysis. For instance, the Program to Evaluate Payment Patterns Electronic Report

(available until January 2009) offers data specific to hospitals. Additional data is available on the state and contractor levels through the Payment Error Measure Rate (PERM) and Comprehensive Error Rate Testing (CERT) programs, respectively. These databases can provide insight on regional problems and focus areas for program-integrity contractors. By using techniques similar to CMS' contractors on a daily basis, improper claims may be identified and corrected more efficiently.

Although, hospitals are encouraged to upgrade their existing data-analysis tools for compliance auditing, the implementation of data mining in hospital management may not be feasible for all hospitals. The additional financial expense and required expertise are barriers, particularly for small hospitals and hospitals located in rural areas. Nevertheless, there are additional audit methods that may be implemented to detect errors if conducted on a regular basis (Table 1).

Table 1: Compliance Auditing Techniques

Monitor the Office of Inspector General (OIG)	• Utilize the OIG 2009 Work Plan. Contractors will use the Work Plan to tailor their data analyses. • Audit a sample of cases associated with patterns of errors to identify the scope of the problem. Under the OIG's Corporate Integrity Agreement Guidance for Compliance Programs, a sample size of 50 is suggested. Conduct a statistically valid audit should your error rate exceed the OIG's suggested 5% error threshold.
Evaluate present on admission (POA) indicator compliance	• Hospitals are required to report one of the five POA indicators to all principal and secondary diagnosis. • Run a coder-specific POA report for one day. • Tabulate results according to the respective POA indicators (Yes→Y; No→ N; Unknown→ U; Clinically undetermined→ W; Exempt→ I). • Ideally, hospitals want a larger number of Y indicators, a low number of N and U indicators. • If there are a high number of U indicators, documentation education may be required.
Evaluate trends of Medicare Severity Diagnosis-related Groups (MS-DRG).	• Evaluate how many discharges hospital has per month for a particular set of MS-DRGs. • Identify anomalies. Were there spikes in a particular MS-DRG from year one to year two? This may indicate a coding error, outlier payment, or medically unnecessary cases.
Evaluate length of stay and discharge status code assignment.	• Hospitals are at risk for billing too-short stays which may signal unnecessary medically admission or stays that are longer however not long enough to justify the assignment of a principal diagnosis. • Hospitals are encouraged to evaluate the principal diagnosis, length of

	stay and number of discharges to identify potential coding or payment errors.

The Fraud Edit Module: What does it mean to hospitals?

The Fraud Edit Module is a project for contractors to develop "a series of edits to deny claims with potentially improper payments." In particular, these edits may help identify improper payments across state borders. Currently, CMS has implemented the use of the Fraud Edit Module for the Medicare Carrier System (MCS) and VIPS Medicare System (VMS). The Fraud Edit Module will be available for the Fiscal Intermediary Shared System in April 2009. CMS is in the process of developing requirements for "a proactive Fraud Edit Module that would allow MCS users to implement on-the-fly edits when potentially fraudulent claims are found locally or nationally." CMS expect that "the [F]raud [E]dit [M]odule will provide Medicare contractors with an improved fraud editing capabilities."

Hospitals may design software to deny claims with potential improper payments associated with a particular therapy or disease (e.g. infusion therapy). Although, software construction may be costly, this technique will assist in ensuring that appropriate claims are submitted to CMS. A less costly method is to "develop a plug and play shared system solution", i.e. a Fraud Edit Module workgroup similar to CMS. The group may consist of representatives from finance, billing, compliance office, and departmental heads to discuss potentially areas of improper claims. A discussion of the hospital's billing risks and the development of methods to address the risks will assist in identifying improper claims prior to submission.

What's Next?

Overall, by 2010 CMS aims to identify and resolve potential vulnerabilities before public disclosure. Additionally, CMS will establish a central warehouse "to collect and synthesize all Medicare program vulnerability data to promote comprehensive and cohesive identification of risks and put more emphasis on developing and evaluating leads." Thus, hospitals should consider implementing similar goals in their compliance programs to ensure compliance with federal regulations.

References

Amato, Jennifer. "Using statistical methods to meet fraud and abuse compliance requirements." HCCA Compliance Today Vol. 10, No. 3. March 2008: 11-13.

CMS, Medicare Program Integrity; Medicare Fraud Edit Module Phase 3, Trans. 265, CR 6135 (Aug. 8, 2008).

"CMS Pours Energy Into Data Analysis, Has Big Plans for 2010." Report on Medicare Compliance Vol. 17, No. 32. September, No. 32 2008: 4-5.

Moran, William, Isnar, Rita, Watt, Sessily. "Medicare and Medicaid enforcement: The planned surge." HCCA Compliance Today Vol. 8, No. 12. December 2007: 10-13.

"New Work Plan Targets Provider-Base Status; OIG Roadmap Has Some Surprises." Report on Medicare Compliance Vol. 17, No. 35. September 2008: 1, 6-8.

"Stakes Raised for Compliance Auditing as CMS Deploys Advanced Data-Analysis Tools." Report on Medicare Compliance Vol. 17, No. 32. September 2008: 1, 5-7.