RAC Monitor: Using Data Mining as a Component of Audit Defense

Andrew B. Wachler. Esq.
Jennifer Colagiovanni, Esq.
Wachler & Associates, P.C.

Over the past several years, the Centers for Medicare and Medicaid Services (CMS) have been focused on preventing and detecting Medicare fraud and abuse more than ever before. With the installment of the permanent Recovery Audit Contractor (RAC) program and the transition to Zone Program Integrity Contractors (ZPICs), methods of preventing fraud and abuse have become increasingly more organized and targeted. Several of these methods revolve around technical innovations as a way to increase efficiency and accuracy when dealing with potential improper claims submitted to Medicare. Of these technological innovations, one of the most prevalent is the increased use of data mining.

CMS has compiled an extensive computerized database of claims and services billed to Medicare by providers. RACs, ZPICs and other audit contractors use this database to analyze the coding and billing practices of Medicare providers across the country. Using this database of Medicare claims, audit contractors identify specific data (e.g. most frequently billed codes, practice location) and use this data to create a model physician profile for that particular provider type. These profiles are then used as a reference point to compare against individual providers' coding and billing practices. This information allows contractors to identify unusual billing patterns, as well as identify outliers by comparing individual provider's billing and coding practices to other providers within the same specialty area. Upon identifying any billing abnormalities or outliers, audit contractors may then take action, such as initiating an audit of the provider's services, in an effort to retrieve any overpayments paid out by Medicare. For example, RACs conduct automated reviews using data mining techniques to identify payment errors (e.g. duplicate claim for the same service), whereby upon discovery the RAC sends an overpayment demand letter to the provider. However, RACs also conduct complex reviews when the contractor determines that a payment error has likely occurred, leading to a request for medical records and further review of the claim.

The audit contractors' use of data mining is a key element of the potential audit risk facing many Medicare providers. If and when an audit occurs, the provider is often faced with significant overpayment demands and the prospect of weathering the five-step Medicare appeals process in an effort to defend against the claim denials. The Medicare appeals process can be ominous and time-consuming. As such, it is imperative that providers proactively prepare to both defend claims on a clinical basis, as well as develop legal challenges as part of the audit defense strategy.

Much like audit contractors, providers can also take advantage of a form of internal data mining. Specifically, as providers challenge audit denials through the Medicare appeals process, they can collect key data elements about the specific claims at issue and the outcome of the appeals at the various stages of appeals process. This data from previously audited claims can then be applied in the defense of current claim appeals.

This approach can be particularly effective for institutional providers including hospitals and health systems which process a significant volume of audit claim appeals. For instance, when appealing claim denials, providers can track specific elements of RAC approved claims and successful appeal results at the redetermination, reconsideration and ALJ stages, and then compare those characteristics with the present appeal case. This comparison may provide additional support and a persuasive analogy in the current appeal where payment was approved in an identical or substantially similar case in the past, giving the provider no reason to know that it would not be approved for the current claim. Such data mining may also serve to bolster a provider's waiver of liability defense, which allows payment where the provider did not know nor could have reasonably been expected to know that payment would not have been made for the services at issue. While appeal decisions in other cases are not binding on ALJs, they may provide persuasive support for Medicare coverage on both the medical necessity of the services and the waiver of liability defense. Providers are advised to redact any protected health information (PHI) on ALJ decisions or information forwarded in similar appeals.

An example of providers using data mining tactics can be highlighted in the RAC denials of inpatient hospital admissions, where the distinction between inpatient and outpatient is often vague and difficult to ascertain. Hospitals can look back at the characteristics of past RAC approvals and successful appeals for individual patients and then draw analogies to the claim details of appeals in progress. The provider should isolate key elements, including length of stay, and primary and secondary diagnoses, type of services, common risk factors, etc., and then use data mining to compare this information to claims approved in the past. Providers are advised to make these data mining considerations early in the appeals process and track favorable appeal decisions at each level of appeal. Due to the early presentation of evidence requirement at the reconsideration stage of appeal, this evidence should be submitted prior to the issuance of a reconsideration decision.

The burden of challenging audit denials through the Medicare appeals process can place a significant strain on providers, making it vitally important for providers to put the necessary tools in place to defeat claim denials. The use of offensive data mining can be an extremely valuable defense tool, aiding providers in successfully appealing RAC, ZPIC, and other audits and ultimately getting their claims approved.