Implementing a Compliance-Based Model of Fraud Risk Control

Legal, Regulatory, and Policy Considerations Continue to Move Compliance Issues to the Forefront

Bill Fox

Health care fraud is complex and comprehensive. Controlling fraud risk requires: (1) technical knowledge of delivery of services, billing practices, physician/hospital arrangements, compliance, and pharmaceutical regulations; (2) understanding of Sarbanes Oxley (SOX), The Committee of Sponsoring Organizations of the Treadway Commission (COSO) and United States Sentencing Guidelines (USSG) corporate governance regulations; and (3) real experience and instinct related to white collar crime, fraud rings, money laundering, prosecutorial priorities and methodologies, internal investigation, and complex litigation.

The most recent Department of Health and Human Services (HHS) and Department of Justice (DOJ) Health Care Fraud and Abuse Control Program Annual Report indicates that during fiscal year (FY) 2009, the federal government won or negotiated approximately $1.63 billion in judgments and settlements and attained additional administrative impositions in health care fraud cases and proceedings. Perhaps more to the point, in FY 2009, U.S. attorneys’ offices opened 1,014 new criminal health care fraud investigations involving 1,786 potential defendants. Federal prosecutors had 1,621 health care fraud criminal investigations pending, involving 2,706 potential defendants, and filed criminal charges in 481 cases involving 803 defendants. A total of 583 defendants were convicted for health care fraud-related crimes during the year. Also in FY 2009, DOJ opened 886 new civil health care fraud investigations and had 1,155 civil health care fraud matters pending.

The ramifications of the Patient Protection and Affordable Care Act and the American Recovery and Re-
investment Act affect every health care entity. The next few years will see an avalanche of regulations and requirements as HHS begins to implement the various pieces of this legislation, and it is a safe bet that virtually every one of these will be fought over tooth and nail, leaving final rules and regulations in flux for years. Fraud risk mitigation will only increase in importance. The paradigm shift in open data exchange, electronic medical record (EMR) adoption, health information exchanges (HIEs), accountable care organizations, and patient-centered medical homes create unprecedented risks in the Health Insurance Portability and Accountability Act (HIPAA), identity theft red flags, and re-identification of protected health information (PHI).

The expansion of the False Claims Act, 31 U.S.C. §3729 under the Fraud Enforcement and Recovery Act (FERA), the influx of 30 million new covered lives created by reform, many from populations traditionally vulnerable to fraud, the globalization of telemedicine, and the general move toward greater and greater transparency brought on by the financial crisis require that health care providers and payors move toward an integrated, front-end model of identity and fraud controls.

Perhaps most importantly, fraud risk implicates patient safety. The silos that currently exist between compliance and post payment fraud investigation are artificial and dangerous. According to the Federal Bureau of Investigation (FBI):

[One of the most significant trends observed in recent health care fraud cases includes the willingness of medical professionals to risk patient harm in their schemes. FBI investigations in several offices are focusing on subjects who conduct unnecessary surgeries, prescribe dangerous drugs without medical necessity, and engage in abusive or sub-standard care practices.]

In June of this year, Dr. Kamal Tiwari was arrested and charged with 11 counts of committing health care fraud that resulted in serious injury to his patients. He is accused of defrauding Medicare and Indiana Medicaid of nearly $21,617,687 between 2002 and 2007. The doctor allegedly asked his patients to undergo unnecessary and potentially dangerous medical procedures like trigger point injections and radiofrequency ablations.

What is needed to prevent this kind of dangerous and costly fraud is implementation of compliance-based fraud risk and identity management programs that reflect more advanced models in health care as well as best practices from other industries. Recent advances in health information technology (IT) enable realistic implementation of these models. Addressing fraud risk via the current ineffective “cops and robbers” system of chasing money after it has gone out the door is no longer a sufficient approach. Financial pressures, reform, and increased enforcement require a fundamental shift, which is now possible. Implementation of identity verification, authentication, and screening mechanisms at the beginning of the payment workflow and HIE are critical to this change.

Compliance professionals, payors, and providers must work with their business units through the challenges of making pre-pay edits and analytics truly effective — workflow, false positives, and prompt pay — in order to bring fraud risk control and real identity management into the compliance framework.

Boards of directors, chief executive officers (CEOs), chief financial officers (CFOs), and general counsels need to understand the business case and return on investment for implementing these changes. The cost of not acting — financial, reputational, and criminal risk — are simply too high to justify inaction. There are reams of white papers out there urging more compliance-based approaches to fraud risk management, but most of the suggested
Implementing a Compliance-Based Model of Fraud Risk Control

approaches are too resource intensive to be implemented into the workflow of an already overly taxed compliance program. Compliance programs often are seen as a cost, and it is up to the compliance leaders within the organization to make the case for implementation of a technology-driven compliance framework that is both comprehensive and cost effective.

**REAL IDENTITY MANAGEMENT — WHO ARE THEY, REALLY?**

A now infamous raid in south Florida of 1,600 licensed durable medical equipment suppliers discovered that 481, virtually a third of those facilities, did not exist. How does this happen? This number does not even address the number that were operating. A sufficient verification check and physical inspection might have revealed providers that have been barred in other states, have ties to convicted felons, are shells for other corporations, or are affiliated with unlicensed practitioners, among other problems. An enrollment/credentialing process could have triggered an alert that would have kept these facilities or providers out of the system, or at least under close surveillance.

Every dollar that does not go out the door is a dollar retained for quality patient care, as opposed to the costly and resource-sapping process of chasing money that is already gone. This is the kind of significant shift in return on investment that is needed to drive implementation of real fraud control.

Increased enforcement of Stark Act violations as well as emerging rules surrounding the formation of accountable care organizations, which require financial relationships between hospitals, providers, labs, imaging facilities, and suppliers to work, means you must have real visibility into the players in your network and the non-obvious relationships between them.

As a compliance officer responsible for the integrity of the providers rendering care to your members (payors), or patients (providers), how can you detect and prevent these types of providers from getting into your network? How can you continuously monitor the providers in your network and be notified when changes occur that would have signaled a problem if present at the outset?

No problem, right? Simply double the resources dedicated to reviewing and investigating providers as they enter your network and order an in-depth review and investigation of every provider currently in your network. Then set up an internal process to monitor every provider’s ongoing legal, criminal, licensure, and facility status. This should involve a significant investment in time from compliance, legal, information technology, business unit leads, then board review and approval.

The above only addresses managing the identities of the providers in your network. What about the members/patients? In some ways this is an even more complex problem. Law enforcement has shown an increasing willingness to pursue fraud cases against patients. At the same time reform demands that you create an online environment that enables patients to access, allow access to others, and in some cases even change certain aspects of their HIPAA-protected health records, all while protecting them from identity theft. A questionable relationship between patient-provider can now be facilitated directly either through an EMR or HIE.

**THE FIRST STEP — WHAT REAL ID MANAGEMENT LOOKS LIKE**

**Tell Us Who You Are**

HIMSS Patient Identity Integrity Work Group’s whitepaper, “Patient Identity Integrity,” makes a compelling argument for the necessity of a national unique patient identifier. Truly effective identity management must be driven off a platform that allows accurate identity resolution and enrichment. This enables accurate linking, analytics, and mining of all data related to a particular patient or entity, regardless
of how “like” that identifying information might be to another’s. This is required for accurate tracking of treatment, prescriptions and testing, disease management, and fraud analytics.

Do You Really Exist? Are You Who You Say You Are?
The next step is to verify the identity. Is the person or provider using the insurance, filling the prescription online, or accessing the EMR remotely really who they claim to be? Wellpoint recently announced it will begin paying for online doctor visits, taking this concept out of the world of concierge medicine and solidly into the real world. Is logging on with a username and password sufficient to establish that it is in fact the patient on the other end of the consultation?

Various forms of multifactor authentication can now be used to ensure the integrity of the identity remotely accessing services, including additional knowledge-based verification, “out of wallet” questions that only the real patient would know. Remote biometrics can be utilized to strengthen this process even further.

Evaluate the Identity
If you have accurate, complete, linked information on the individuals and entities utilizing your network, now is the time to evaluate them — not after they take advantage of your lack of visibility into who they really are and how they are connected. The system should validate the identity against business rules, legislation, and regulations to determine if this person or entity is qualified to engage the present transaction. Optimally, particularly at enrollment, the identity should be checked against criminal, sanctions, licensing, and other public records to determine if there is an issue that they did not disclose, despite new rules requiring them to do so.

Risk Alert
Finally, based on each of the steps, the system should either efficiently process the transaction or notify you through an alert that this identity appears to create a risk in this context. A major gap in identity security in many organizations is ongoing monitoring of relevant data that would affect eligibility to participate. Identity management should include ongoing monitoring and include a system to alert the organization when data related to an identity indicates a new risk.

A Layered Approach to Front End Fraud Risk Avoidance
Your compliance program seeks to put in place processes and protections that prevent potentially costly mistakes and violations from occurring. The current paradigm in health care fraud “prevention” is to mine data after the money has already gone out the door, investigate potential fraud, then go through the very resource-intensive, time-consuming, expensive, and often unsuccessful process of trying to get it back. The fact that this method actually has a very respectable return on investment, estimated to be approximately $7 recovered for every $1 spent, demonstrates both the strength of the best post-payment rules-based systems and the tremendous opportunity that exists to vastly improve the paradigm, and return on investment, by migrating this process to the front of the payment workflow.

An optimal system would take a layered approach to eliminating the main obstacle to present attempts to implement pre-pay systems, resource sapping false positives, and the problems with prompt pay and work flow that follow. A claim that is improperly flagged and pulled off the payment track for investigation that turns out to be fine and is returned for payment after a significant delay is costly. Many states’ prompt payment regulations impose significant fines on claims that are paid late, in some cases as little as 15 days after they are submitted.

The first step in implementing an effective pre- and post-pay fraud risk control en-
Implementing a Compliance-Based Model of Fraud Risk Control

...environment is instituting an end-to-end, continuous ID management process as set forth earlier. By first flagging or scoring claims that involve an identity that has been tagged as high risk, the organization takes the first step in preventing money from going out the door connected to a bad claim.

Rules-based fraud detection systems that chunk through claims and identify outliers are a key piece of a pre-and post-pay fraud risk control environment. Migrating this process, which currently occurs almost exclusively at the back end, to the front end, is critical to changing the game in favor of the payors and providers that are giving proper care and attempting to pay legitimate claims as efficiently as possible. Going beyond simply looking at claims and including analysis of clinical data in this process would refine it even further. Providers feel crushed under the pressure of multiple government programs intended to audit them and find overpayments and fraud: zone program integrity contractors, Medicare drug integrity contractors, Medicaid integrity contractors, and recovery audit contractors all exert tremendous pressure and expense on providers trying to prepare for audits, record requests, and demands for overpayments. The best way to change the dynamic is to prevent payments from being made that will later cause problems with one or more of these Centers for Medicare & Medicaid Services (CMS) contractors.

Law enforcement also has significantly increased its efforts in prosecuting health care fraud. Provisions in the Patient Protection and Affordable Care Act (PPACA) make it significantly more dangerous to pay claims without pre-payment visibility into the risk attached to them. For example, an overpayment retained for more than 60 days is deemed to be an “obligation” for purposes of the False Claims Act. PPACA amends the health care fraud statute (18 U.S.C. §1347) to provide that, “with respect to violations of this section, a person need not have actual knowledge of this section or specific intent to commit a violation of this section.” In other words — what you don’t know can hurt you. Therefore, it is crucial that investment in the technological, policy, and business workflow issues associated with shifting to pre-payment fraud detection be made and begin immediately.

Once a claim has been scored for risk related to the identity and the actual contents of the claim itself by rules-based algorithms, it should be run through a predictive analytics tool to determine if there are non-obvious aspects of the claim that require immediate further review. The promise of predictive analytics to detect fraud in health care for the most part has been unfulfilled. Initially, it was hoped the kind of predictive analytics utilized so successfully in the credit card industry would simply shift directly over and start doing the same thing for health care. The complexity, variability, and “dirty data” involved in health care have hindered that from happening in the way that was hoped.

The key problem to date has been far too many false positives. A false positive is a claim flagged as problematic that turns out to be legitimate after a time-consuming manual review. Pulling these claims out of the payment workflow only to find they are payable causes significant problems, the most important for payors being penalties associated with late payment, and for providers, not getting payed on time.

There are two ways to address these issues. Both must be employed because predictive analytics are simply far too important to ignore. In much the same way that inevitability pre-payment fraud detection has been talked about for years, and almost daily since the reform debate began, predictive analytics simply must become part of the review of every claim before it is paid.

The first way is to explore various statistical models to determine those models that can keep false positives to an acceptable minimum. This is not the forum, and the author lacks the technical knowledge, for a treatise on statistical modeling. That said, as more companies enter this market with
Implementing a Compliance-Based Model of Fraud Risk Control

experience from other industries, particularly those that involve modeling of medical claims in other contexts, more and more varied models will be tried on health care data, and we can begin to move toward predictive models that satisfy the requirements for low false positives that will allow inclusion at the front end of the payment workflow.

The second way is to take a layered approach to analyzing data — what could be referred to as “automated triage.” Resources will always be the key issue in pre-payment fraud control. When a claim is flagged, unless it violates an absolute rule, the most expensive resource of all, a skilled person, needs to look at that claim and make a judgment about it.

By taking a layered approach to pre-payment fraud control, the results that reach that skilled person's desk can be refined so that they deal with less and less “noise” and more “signal.” Going forward the problem will never be the amount of data and content, it will always be decreasing the volume of content that a person deals with while increasing the quality of that content. By combining identity and entity resolution, rules-based claim and clinical review, complex linking analysis, and predictive analytics into a seamless work-flow, we will come closer and closer to the reality of an integrated pre-pay fraud risk control environment.

CONCLUSION — WHEN AND HOW

It is an interesting time to be a compliance professional. Legal, regulatory, and policy considerations, and the evening news, are moving compliance issues from the back room to the congressional hearing floor. Health care reform has created an atmosphere of flux. One thing that is clear is that taking a reactive approach can only spell trouble for your organization. “We did not know” is an answer that no longer flies with law enforcement or the board of directors. Cutting edge technology is opening up new possibilities to put in place more effective controls to deal with the multitude of new pressures. Hopefully, this article has introduced you to some information and concepts you can proactively explore to ensure that your organization stays ahead of the curve.

Endnotes:
2. Sec. 6402 PPACA.
3. Sec. 10606 and 6402 PPACA.