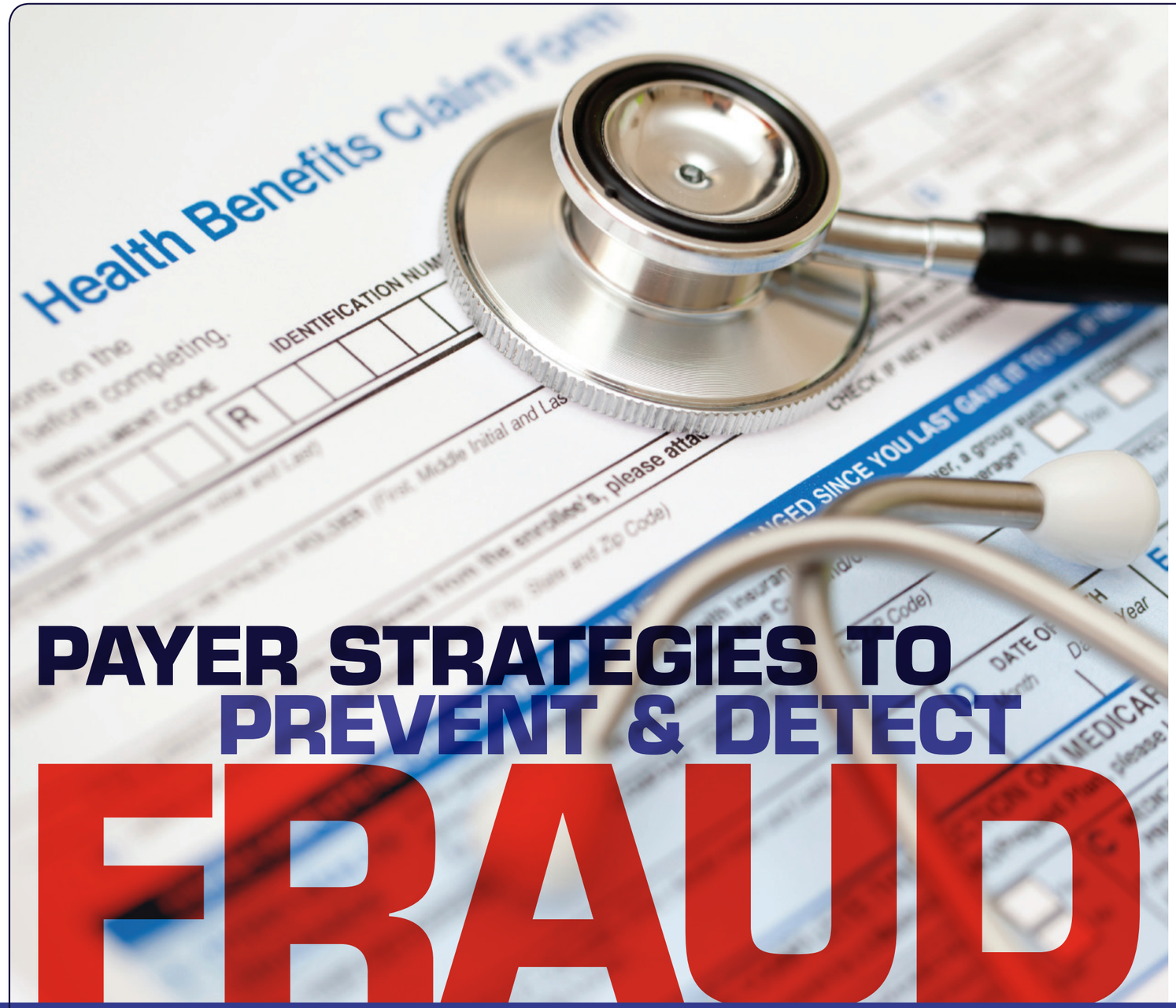
FierceHealthPayer
TWICE WEEKLY NEWS FOR HEALTHCARE PLAN EXECUTIVES



PAYER STRATEGIES TO PREVENT & DETECT FRAUD

▶ With billions of dollars at risk, preventing losses and recouping revenue from fraud, waste and abuse is one of the most difficult challenges U.S. healthcare payers face. In addition to severe financial losses, scams and schemes threaten insurers' most valuable resource—members' health and safety.

Health insurance fraud costs roughly $234 billion a year, according to the National Health Care Anti-Fraud Association. Small health plans that successfully deploy anti-fraud programs can save $5 million ($2.70 per enrollee), while medium-sized plans can save about $10 million ($1 per enrollee), **according to America's Health Insurance Plans**. Large health plans could retain up to $300 million ($3 per enrollee).

Although the majority of healthcare payers are still employing the pay-and-chase method of trying to recoup money after they've paid claims, advances in health IT and data analytics are allowing payers to be more proactive.

But these same advances also are aiding criminals. And schemers are becoming more sophisticated—finding ways to exploit the new ICD-10 coding system, for example.

We interviewed several payer executives and fraud experts for this special report. All of them stressed many of the same key concepts:

- Leverage technology with careful management and testing
- Commit plenty of time and resources—including leadership attention and staff training—to fraud prevention
- Collaborate with law enforcement, providers and enrollees
- Stay current on the latest examples of insurance fraud in the news to stay ahead of the game.

The advice, guidelines, and best practices contained in this eBook are designed to help payers protect their bottom line, as well as member's health. ●

Karen M. Cheung /// Editor /// *FierceHealthcare*

▼THANK YOU TO OUR SPONSOR

tableau SOFTWARE

FierceHealthPayer
TWICE WEEKLY NEWS FOR HEALTHCARE PLAN EXECUTIVES

Best Practices to Protect Your Company from Fraud

BY J.M.K. ANTONIO


If you see providers who deviate from the norm, review further to determine what's driving the high numbers.

▶ The schemes are legion: Claims arrive for fake lab tests or for medical equipment that was never ordered. Addicts doctor-shop for prescriptions or find pill mills and overdose. Illegal aliens and organized criminals infiltrate provider networks and bill for services that were never provided. Every benefit is vulnerable to exploitation. Significant losses follow; some schemes are so fast and furious they can bleed payers out of millions in less than two months.

How do insurers guard against those who plot to take the money and run? Experts reveal the following effective anti-fraud practices, all of which rely on dynamic and visible special investigations units.

PREPAY DEFENSES

Fraud recoveries return about 20 cents on the dollar—not paying fraudulent claims nets dollar-for-dollar savings. So Alanna Lavelle, director of investigations for southeast and central regions at WellPoint, trains employees to stop money from going out the door through prepayment review.

Unlike the traditional pay-and-chase method, prepayment review requires problem providers—including aggressive billers who refuse to change their habits—to file paper claims that clinicians and coders then process with special attention.

"Even if you put two providers on prepay, it could save a million dollars if they file large claims."

ALANNA LAVELLE, DIRECTOR OF INVESTIGATIONS FOR SOUTHEAST AND CENTRAL REGIONS, WELLPOINT

It's "one of the best ways to counteract fraud," says Christine O'Neil, a supervisory special agent at the Boston FBI's Health Care Fraud Squad. Lavelle elaborates: "Even if you put two providers on prepay, it could save a million dollars if they file large claims."

O'Neil also recommends staying current with the latest schemes by following news reports of fraud. Another tactic: Run claims queries to gauge vulnerability and cross-check claims when services require specific diagnoses to qualify for payment. For example, if podiatric services are only covered for diabetics, verify diabetes diagnoses before paying claims.

DATA ANALYSIS ON A SHOESTRING

Special investigations units undoubtedly require vigorous data analytics to determine fraud risk, but what if a state-of-the-art data solution isn't affordable? Darrell Langlois, vice president of compliance, privacy and fraud at Blue Cross and Blue Shield of Louisiana, shares a low-cost data analysis idea to find probable cases.

"With any specialty in any fraud scheme, there are four ratios," he says. "By simply putting two numbers one over the other, generating a ratio, and then matching those numbers provider by provider, you can determine who presents themselves as vulnerable to committing fraud." The ratios are average dollars paid per patient, average visits per patient, average dollars paid per medical procedure and average medical procedures per visit, he says. If you see providers who deviate from the norm (e.g., if a given provider averages eight office visits per patient annually while other providers in the same specialty average two visits per patient a year), review further to determine what's driving the high numbers.

LEVERAGING IN-HOUSE RELATIONSHIPS

Efficient special investigations units build strategic internal networks, and the resulting visibility can raise fraud awareness. Besides medical management, legal and IT teams, consider connecting with stakeholders whose roles don't typically include fraud-specific duties:

- **Board of directors:** Special investigation reports that reach board audit committees often prompt management to respond faster to fraud threats.
- **C-Suite:** Investigators who earn leaders' trust gain valuable top-down support. Successful private payer investigations units know what leaders expect and align with corporate anti-fraud strategy.
- **Provider network representatives:** "Given today's fraud schemes, if you don't control your provider network, you will be vulnerable," Langlois says. Rigorous audits of participating providers ensure the integrity of your network.
- **Other associates:** Offer recognition and incentives for good fraud tips from employees. For instance, WellPoint showcases these referrals in anti-fraud trainings for staff.

COLLABORATION WITH LAW ENFORCEMENT

Special investigations units that work closely with law enforcement are more likely to get leads on cases that can lead to prosecution and create a sentinel effect. To improve collaboration with law enforcement, Lavelle hires former law enforcement employees.


If podiatric services are only covered for diabetics, verify diabetes diagnoses before paying claims.

FierceHealthPayer
TWICE WEEKLY NEWS FOR HEALTHCARE PLAN EXECUTIVES

Law enforcement personnel vary greatly in personality, depending on the area or agency, Langlois notes. He recommends accommodating their sensitivities and getting comfortable with them by interacting before case work begins.

O'Neil reminds payers that FBI referrals are just the start of an investigation. Build on the referral by documenting the suspected fraud and include essential evidence, such as copies of interviews, in the case files.

"We involve law enforcement long before the case is ready [to] report," Langlois says. "Allowing law enforcement to see what a case is about and digest the facts in person allows them to build … true interest in bringing prosecution. Their passion then translates well to the prosecutor, who can raise issues that can be addressed while time is left to do so. I have heard complaints about payers just writing reports and turning [the case] over. This is not a good practice. Getting to know the agent and prosecutor allows for the best results."

"If you don't control your provider network, you will be vulnerable."

DARRELL LANGLOIS, VICE PRESIDENT OF COMPLIANCE, PRIVACY AND FRAUD, BCBS OF LOUISIANA

WORKING WITH PHARMACY BENEFITS MANAGERS

Pharmacy benefits managers can do more to fight fraud than monitor excluded provider services. Debra Devereaux, vice president of pharmacy for Gorman Health Group, in Washington, D.C., recommends contractually requiring pharmacy benefits managers to report high narcotics use and ensure that network pharmacies and are not under action by state boards. Pharmacy benefits managers should also ensure that network pharmacies employ pharmacists licensed to practice in their states and attest annually that all participating pharmacies have completed employee anti-fraud training.

CUSTOMER EDUCATION AND PROTECTION

O'Neil also stresses the need to educate customers about fraud. Teach them to read explanation-of-benefits forms and to report unfamiliar items. Remind them to safeguard their member numbers and ID cards and explain how medical identity theft can affect lifetime maximums and future service access, as well as their own safety.

Lavelle recommends giving top priority to and intervening promptly in schemes that threaten patient safety. "We see it as our role to protect members," she says.

Langlois agrees. "There are many cases nowadays of someone committing healthcare fraud and, in the course of that, physically and irreparably harming patients. That's the epitome of why this crime needs to be stopped." ●

FierceHealthPayer
TWICE WEEKLY NEWS FOR HEALTHCARE PLAN EXECUTIVES

BCBSNC Interview: Combat Fraud at Point of Care

BY KAREN M. CHEUNG

▶ Although the industry tends to think of fraudsters as masked criminals hiding behind bogus storefronts, seemly innocent, sick patients also can be the perpetrators of fraud, bilking the system by using others' identification. *FierceHealthPayer* spoke with Gary Crispens, director of special investigations unit (SIU) at Blue Cross and Blue Shield of North Carolina (BCBSNC) to hear what anti-fraud steps the insurer is taking to combat scams at the point of care.


Gary Crispens

Q: How does BCBSNC conduct anti-fraud efforts and what's the return on investment?

A: The special investigations unit (SIU) at BCBSNC uses a state-of-the art fraud detection software to mine claims payments and other data to identify outliers for additional investigation. Outliers are identified by a variety of analytics based on payment data, utilization and billing patterns, the provider's practice specialty profile and mathematical formulas.

SIU uses the industry standard of an 8:1 return on investment as one of its performance measures. The ROI is measured by the actual cost of the SIU, compared to actual cash recoveries, savings that result from prepayment claims reviews and denials, as well as savings from educating providers that correct their billing practices.

Q: What do you do to prevent fraud perpetrated by patients at the point of care?

A: Providers are the first line of defense against point of care fraud, and taking the extra steps to verify the identity of the person is a best practice. We encourage our network providers (doctors and pharmacies) to obtain accurate patient identification at the point of care, such as dates of birth, member home addresses, phone numbers and middle initials as part of the patient verification process. We also advise providers to ask members for a photo ID.

"Repairing medical history is just as difficult as repairing a stolen credit history and can create financial hardships when providers try to collect for fraudulent changes."

We also encourage members to make sure their physicians ask them for a picture ID, and remind them to treat their healthcare ID card as they would a Social Security card, a credit card or their driver's license [by securing it]. We inform them the sharing of healthcare ID cards can lead to mixed medical histories, which can result in potential life-threatening situations, such as receiving medications they are allergic to or [receiving] inappropriate treatments. This is especially important in an emergency medical situation.

SIU works closely with BCBSNC's corporate pharmacy department and the pharmacy benefit manager to identify and respond to potential doctor shoppers. We contact prescribing doctors to make them aware that more than one provider is prescribing potentially addictive medications. In some cases where the abuse is excessive, we send referrals to our law enforcement investigative partners.

Q: What tactics are most effective at detecting and preventing fraud and abuse?

A: The most effective detection method is being aware of fraudulent scams in the industry and staying on top of new trends.

The lasted trend was recently featured on national television news where "crooks" are obtaining a person's identity to file false income tax returns for a refund. One payment option for the income tax refund is to receive a prepaid debit card that is then quickly converted into retailer gift cards and money orders. [Schemers] are bribing employees in assisted-living facilities to obtain residents' identities and bribing employees in healthcare offices for patient data. They are also breaking into doctor and dentist offices to steal patient records that can be assisted by people that go to work for the provider. False healthcare providers that have "free services" are also a method being used to gather identity information.

In addition to networking with the National Health Care Anti-Fraud Association, SIU is very active in the Blue Cross Blue Shield Association's National Anti-Fraud program, which provides anti-fraud strategies and fraud education materials. They have conference calls where new fraud techniques are discussed, along with lessons learned from successful investigations and prosecutions.

"Providers are the first line of defense against point of care fraud, and taking the extra steps to verify the identity of the person is a best practice."

The Association coordinates cases across state lines by providing confidential alerts when certain providers are under investigation by state and federal agencies. This may result in companies providing payment information to assist in the prosecution. It could also result in placing the provider on a prepayment review to ensure the payment is supported by evidence of medical necessity.

We also use an industry-leading fraud detection software to proactively look for questionable billing practices and patterns to determine root causes of complicated frauds and implement corrective/preventative measures. For example, the software provides a profile of the number of patients seen by a provider on a daily basis. This will show if the provider was paid for more patients than could actually be seen on a given day, which would trigger an investigation.

When an investigation is opened, you never know which direction it might take. It can include additional people being involved beyond what was initially thought, complicated bribery and kickback schemes or other family members being involved. Learning from successfully prosecuted cases and how the fraud was discovered can lead to additional system controls, prepayment reviews, investigator education and awareness or enhanced data-analysis techniques.

Q: What advice about preventing fraud and abuse would you give to other payer organizations?

A: Everyone has a role in preventing healthcare fraud. Subscribers need to be educated on their role and how to identify and report suspected fraud. Providers need to be vigilant in validating the identities of patients, securing medical records to prevent medical identity theft and accurately bill only for those services that have been rendered. Payer organizations need to stay informed on current fraudulent practices and preventive measures by networking with other anti-fraud professionals. ●

Editor's note: This interview has been edited for length and clarity.

FierceHealthPayer
TWICE WEEKLY NEWS FOR HEALTHCARE PLAN EXECUTIVES

How ICD-10 Will Impact Your Anti-Fraud Efforts

BY LIISA SULLIVAN

▶ There's been much discussion that ICD-10 may actually help ramp up fraud detection by reducing ambiguity and misinterpretation due to greater code specificity. The logic of ICD-10 facilitates tools that can be used to detect questionable patterns and suspected fraud. But risks do exist.

Blue Cross and Blue Shield of Illinois is scrutinizing three key areas, says Sydney V. Ross-Davis., medical director of special investigations:

- **Assessing ICD-9 data:** Assess how to leverage ICD-9 information to ICD-10 and identify codes that may present the greatest risk.
- **Unique provider structure:** Understand and accommodate each unique provider's approach to clinical coding, medical records and billing systems.
- **Expert training:** Train external-facing staff to identify and appropriately triage provider problems and questions to the correct levels of expertise.

Immediately following the October 2014 compliance date, there will be a transitional period of 12 to 24 months where providers become more "fluent" in using ICD-10.

"During this time, it will be difficult for payers to differentiate between an error and a fraudulent claim," says David Biel, principal in Deloitte's health plans technology practice in Chicago. "Provider coding patterns will take time to become predictable. Therefore, this transitional period represents a higher risk time for payers and targeted steps will be required to guard against this."

For instance, fraud detection mechanisms will need to change. Payers use numerous techniques to detect fraud and abuse, from retroactive claims reviews to statistical analysis. Each strategy requires sophisticated algorithms to identify abusive patterns, such as submitting claims for phantom procedures, billing for visits that never took place or upcoding. It's critical to understand how the detection algorithms are impacted as a result of the expanded code set, he says.

Some algorithms may use the ICD-9 code set; some may not. Just as claims adjudication systems must be converted to "speak" in ICD-10, so too, must fraud and abuse systems. Some payers have built their own fraud-detection capabilities which must be analyzed and remediated for ICD-10. Others use vended software that will need to be upgraded by the vendor and configured in the payer's environment based on their fraud and abuse risks.

"With proper planning, health plans, providers and vendors can greatly mitigate risk."

SYDNEY V. ROSS-DAVIS., MEDICAL DIRECTOR OF SPECIAL INVESTIGATIONS, BCBS OF ILLINOIS

All of this work requires a detailed understanding of ICD-10 and the functional systems used to detect fraud by testing through an ICD-10 paradigm. Adequate funding and resources must be allocated.

"If not done, payers will have trouble identifying provider mistakes, when their systems are erroneously identifying or not identifying fraudulent behavior, and when fraud is actually happening," Biel explains.

IDENTIFY TOP RISKS

Typically, fraudulent activity is detected by keeping an eye out for non-conforming diagnoses in claims. But the sheer complexity and volume of codes makes ICD-10 much easier for unscrupulous providers to hide behind, says Scott Strain, Special Investigation Unit department supervisor at Dean Health System, one of the largest integrated healthcare delivery systems in the country.

Biel identifies two ICD-10 hot spots to warrant close scrutiny:

- **Information management:** Most payers have large data warehouses, data marts and extensive infrastructure and processes, churning out thousands of reports for many uses (i.e., operational, and trend analysis). Many of these will be impacted. And since this data has multiple uses, requirements and often complex scenarios that impact payment and/or member health, it's critical to allocate time, resources and dollars to understand and analyze the problem, Biel says. Payers should approach information management as a medium-to-large size program with a full requirements phase followed by a design and solution phase to address individual requirements. There is no one-size-fits-all technical solution such as a crosswalk.
- **Testing:** Many payers falsely assume that testing ICD-10 will be similar to other past testing efforts. ICD-10 impacts many processes, systems and people and traditional methods may be overwhelmed which begs the

VALUABLE RESOURCES FOR A SMOOTH TRANSITION

- Health plans will need a variety of resources to accommodate the ICD-10 transition. They should include:
- A comprehensive platform to communicate clear, consistent and concise messages to providers
- A data-mining tool
- Trained data analysts
- Professional clinical coders
- Physicians with strong clinical and coding expertise
- Training programs for internal and external audiences
- Translation tools to go from ICD-9 to ICD-10 and from ICD-10 to ICD-9
- A comprehensive fraud abuse risk mitigation program
- Evaluation and measurement processes and protocols which are consistent, transparent, reference sound clinical practice, leverage correct coding guidelines and grounded in good investigatory practices

FierceHealthPayer
TWICE WEEKLY NEWS FOR HEALTHCARE PLAN EXECUTIVES

need for a risk-based approach that focuses on the most critical areas that have changed first, and ensuring those are sound before tackling other areas.

Additional risks include:

- Not using clinical scenarios for test data
- Not analyzing existing IT systems
- Limited collaboration

MITIGATE TOP RISKS

"We've been talking for a long time about payer/provider collaboration; it's a critical step to mitigating risk in fraud and abuse and overall ICD-10 readiness," Biel says.

Collaboration takes the form of early-adoption programs by providers and payers, creating joint payer/provider testing programs, and working together to drive readiness. This will have several benefits including:

- Drive a faster adoption of ICD-10 and accelerate the learning curve for providers
- Root out claim processing issues for payers based on real ICD-10 claims that are coded by providers
- Test fraud detection mechanisms in payers to determine if they are functioning as expected
- Work together to determine where errors and issues are occurring, as a combined provider/payer team, before going live
- Open the lines of communication to improve the overall relationship

"With proper preparation, planning, communication, testing, and evaluation methods in plans, health plans, providers and vendors can greatly mitigate risk," says Ross-Davis. For example, the Enterprise Special Investigations (ESI) unit at Health Care Service Corporation (HCSC), which owns Blue Cross Blue Shield of Illinois, Oklahoma, New Mexico and Texas, works closely with Blue Cross Blue Shield of Illinois' Medical Management Department to investigate medical fraud and abuse, he says.

"This team has taken the necessary steps to develop a mitigation program to combat potential fraud and/or abuse," he says. "Prior to the 'go-live' date for ICD-10, the ESI Department will institute detailed training programs, develop newly refined approaches to the analysis of trends in submitted claims and continue to investigate aberrant billing and provider or member practices." ●

"During this time, it will be difficult for payers to differentiate between an error and a fraudulent claim. Provider coding patterns will take time to become predictable. Therefore, this transitional period represents a higher risk time for payers and targeted steps will be required to guard against this."

DAVID BIEL, HEALTH PLANS TECHNOLOGY PRACTICE PRINCIPAL, DELOITTE

6 Steps to Prepare for and Survive a Federal Fraud Investigation

BY J.M.K. ANTONIO

▶ While payers are busy identifying fraudulent providers and members, they sometimes find themselves at the receiving end of a federal fraud investigation that can take several years, and precious resources, to resolve.

Consider Wellcare Health Plans, Inc. The Florida-based HMO agreed in April to pay $137.5 million to settle whistleblower allegations that company executives discussed ways to double-bill Medicare and Medicaid – following years of investigation. The WellCare case dated as far back as 2006, when a senior financial analyst for the company made secret recordings of executives allegedly talking about how they could bilk Medicare. After an FBI raid a year later, the case continued to make headlines until April 2-12, when investigators announced that the whistleblower would receive about $21 million for his efforts.

Though investigations vary in scope, it pays to recognize the real risk that fraud poses and work proactively to mitigate it—before, during and after a federal investigation.

BEFORE AN INVESTIGATION: LAYING THE GROUNDWORK

1. Strengthen compliance monitoring

Kirk Nahra, partner in the Washington, D.C.-based law firm Wiley Rein, advises insurers to improve their compliance programs with ongoing assessment. "You need to be identifying compliance risks and checking yourself on a regular basis," he says.

Pay attention to fraud issues in the industry because the government pursues copycat cases. "There's a history in the healthcare industry. Fraud can involve just one company, but actions that lead to fraud often are repeated among similar players in the industry," Nahra says.

A robust compliance program also can position companies to negotiate gains. A company might be allowed to investigate itself in response to fraud allegations or reach a compromise for records production, and prosecutors might disclose False Claims allegations and allow the company to present its side of the story.

2. Investigate all complaints

Effective compliance programs investigate and act on employee complaints. Keep in mind that any reported employee concern

"There's a history in the healthcare industry. Fraud can involve just one company, but actions that lead to fraud often are repeated among similar players in the industry."

KIRK NAHRA, PARTNER, WILEY REIN,

involving government business can morph into a False Claims case. Staff can become whistleblowers if their concerns aren't heard.

Nabil Istafanous, principal at Corporate Counsel Solutions in Seattle, experienced a federal civil fraud investigation while serving as chief compliance and ethics officer at a regional health plan. Though the local U.S. Attorney's office declined to intervene in the qui tam case, the investigation spanned several years.

"I wish I had known that, despite my instincts that we had done everything possible to address the employee's concerns and therefore must have resolved the issue, that I should be prepared to address the same questions years later," Istafanous reflects. "Fortunately, we thoroughly examined the issues when concerns were raised and addressed operational weaknesses with a corrective action plan shared with regulators."

Istafanous's experience underscores the need to take all reports of wrongdoing seriously – and

"The more transparent and forthcoming you are, the better your treatment. It's that simple."

MARIANNE JENNINGS, FORMER REGULATOR

to document your response. "If concerns raised are specific and credible, you should appropriately review those concerns, even if that means hiring outside experts at considerable expense." he says.

3. Build an ethical culture

Help employees build integrity into everything they do – from the way they manage records to how they deal with third parties. Consider these tips:

- Translate vague concepts of ethics and integrity into specific behavioral requirements for staff.
- Educate staff about the rules regarding discoverable email.
- Distribute anonymous integrity surveys and scrutinize the results. Answers to open-ended questions can expose early-stage regulatory issues. For example, if surveys show that staff misunderstand a government-reporting procedure, payers can take swift remedial action.

DURING AN INVESTIGATION: COORDINATION, CARE AND CANDOR

4. Assemble a qualified legal team

When an investigation begins, assemble a legal team to coordinate and respond to demands. Choose lawyers who specialize in corporate integrity issues and who understand the context and history relevant to the facts. In False Claims cases, Istafanous recommends that the legal team treat prosecutors "not as opposing counsel, but as the judge who weighs the credibility of the qui tam relater against the credibility of the company and its counsel."

5. Support staff and be transparent

Address employees' fears during the investigation, such as their worries about job loss and incriminating themselves or the company. Decide whether to provide counsel to represent employees at the company's expense. Inform staff of the investigation's progress to the extent possible, keeping in mind limits on disclosure. What's important is that the company not stay silent on the case. Companies need to fight the tendency to clam up and instead provide periodic reassurances to staff.

Coach your staff to preserve documentation, turn over evidence and answer questions truthfully.

"As a former regulator, I know this: the more transparent and forthcoming you are, the better your treatment. It's that simple," says Marianne Jennings, a longtime authority on business ethics and emeritus professor of legal and ethical studies at Arizona State University.

AFTER AN INVESTIGATION: CONSTANT VIGILANCE

6. Don't let your guard down

Even if your company receives a clean bill of health after an investigation, don't breathe a sigh of relief just yet. Analyze the experience. What could have been handled better? What must change? Did employees' behavior in the case or investigation violate ethical standards? If so, pursue disciplinary action as necessary.

Finally, remember there still may be problems even if investigators find no regulatory violations. "Regulators visited Bernie Madoff's shop three times, and there was no disciplinary action," Jennings says. "Advise the board and management team to keep an eye on whatever it was the regulators looked at to see if something evolves afterward." And continue compliance monitoring, as new fraud risks continue to make headlines. ●

"If concerns raised are specific and credible, you should appropriately review those concerns, even if that means hiring outside experts at considerable expense."

NABIL ISTAFANOUS, PRINCIPAL AT CORPORATE COUNSEL SOLUTIONS