Medical Practice Compliance

News, tools and best practices
to assess risk and protect physicians

ALERT

June 27, 2011 | Vol. 23, Issue 12

IN THIS ISSUE

Proposed HIPAA rule goes beyond law's requirements 1

Claims analysis tool may help CMS catch fraud faster 1

Keep compliance records confidential to reduce your risk 2

Facebook gaffe costly for one doctor 3

Agencies team up to nab company for false claims and HIPAA 4

4 ways to prepare to account for disclosures 5

Case 61: The case of the risky incident-to services 7

Proposed HIPAA accounting for disclosures rule packs a compliance wallop

You would face new compliance hurdles under the long-awaited proposed changes to HIPAA's accounting disclosure rule, published in the *Federal Register* May 31. You would also have to deal with more patients asking for such disclosures than ever before.

The new rule implements changes mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act passed in 2009, which expands a patient's right to an accounting of disclosures of his or her health records to carry out payment, treatment and health care operations when an electronic health record is used. HIPAA had originally exempted such disclosures from the accounting requirement.

*(see **HIPAA**, pg. 5)*

New claims tracker aims to help CMS spot fraud faster

Your claims will face a new type of scrutiny starting July 1, when CMS deploys new predictive modeling technology to find fraud faster. The agency announced the program June 17. The technology is similar to that used by credit card companies.

The modeling technology will help identify potentially fraudulent Medicare claims nationwide and stop those claims before they're paid, CMS officials said in a statement.

Example: If a provider files a claim using the identification of a Medicare beneficiary who's dead, that would raise a red flag under the new technology, says Tony Salters, a CMS spokesman.

CMS selected government contractor Northrop Grumman to deploy algorithms and an analytical process to analyze CMS claims by patterns such as beneficiaries, providers or service origin to identify potential problems and assign an "alert" and "risk scores" for those claims, CMS officials said in the statement. Zone Program Integrity Contractors (ZPICs) will have access to the results to help develop

*(see **tracker**, pg. 8)*

Cut your risks by keeping your compliance records confidential

You know that an effective compliance program includes investigating complaints, conducting audits, keeping lines of communication open and documenting your compliance efforts. But don't let everyone in your office access all of that information, or you'll open yourself up to additional compliance woes.

While HHS's Office of Inspector General's (OIG's) voluntary compliance guidance for physicians does not say whether or how to keep compliance information confidential, it's a best practice to do so, according to David Zetter, president of Zetter Healthcare Management Consultants in Mechanicsburg, Pa., who trains physician offices in compliance.

The guidance suggests only that you use a process to allow those who report a compliance concern to be anonymous and do as much as possible to maintain the anonymity of those named as possibly involved in noncompliant conduct.

"You can never promise confidentiality, but use lock and key and 'certain eyes only'," Zetter suggests. **Example:** If much of the office knows about a fraudulent billing investigation or a sexual harassment allegation, you are exposed to defamation claims from the alleged perpetrator, whistleblower suits from other staff members, or employee discrimination claims, he warns. Any patient information involved that is not kept confidential could trigger a HIPAA violation, warns consultant Wayne van Halem, president, the van Halem Group, Atlanta.

Unfortunately, many practices are lax when it comes to keeping compliance records confidential. Even the most scrupulous of compliance officers often have little privacy in a physician practice. They often share work, desk and file space with others in the practice, allowing access to those who shouldn't have it.

The confidentiality requirement is not absolute. You'll find it necessary at times to share the information in a compliance record, although there are no hard and fast rules. "There are so many different variations on what to keep confidential. It depends on what you're dealing with," warns Zetter.

"Hopefully this will be more clear cut when we get guidance [about mandatory compliance programs] under the Patient Protection and Affordable Care Act, where it's expected that confidentiality and privacy will be addressed," says van Halem.

In the meantime, use these six guidelines to help you wade through this quagmire:

Subscriber Services

Editorial:
Scott Kraft – 1-301-287-2361 *skraft@decisionhealth.com*
Marla Durben Hirsch – 1-301-299-6155 *mhirsch@decisionhealth.com*
Chris Huntemann – 1-301-287-2722 *chuntemann@decisionhealth.com*
Sean Weiss – vice president, DecisionHealth Professional Services
sweiss@dhprofessionalservices.com

Marketing:
Elise Yore – 1-301-287-2274 *eyore@decisionhealth.com*

Subscriptions:
For direct questions about newsletter delivery and account status, please contact DecisionHealth® at 1-877-602-3835, or email us at: *customer@decisionhealth.com*

Compliance Listserv:
To join our free Internet forum on fraud and abuse issues, go to *http://listserv.ucg.com/cgi-bin/listserv/listserv.pl/fraud-l*, click on the "Join the Fraud & Abuse Discussion Group" link, and follow the instructions.

Reprints:
To request permission to make photocopy reprints of *Medical Practice Compliance Alert* articles, or to obtain information on our copyright waiver, multiple copy and site license programs, please call us at 1-866-265-0148, or email Gary Belski at: *gbelski@decisionhealth.com*.

Medical Practice Compliance Alert **is published 24 times per year by:**

DecisionHealth® (a UCG company)
Two Washingtonian Center
9737 Washingtonian Blvd., Suite 100
Gaithersburg, MD 20878-7364

ISSN: 1047-1863
Price: $547 per year
DecisionHealth®, LLC

1. **Require confidentiality by all employees**. Have employees sign confidentiality agreements covering the operations and compliance issues of your practice. This helps preserve confidentiality if an employee inadvertently sees or overhears a compliance report or other record he shouldn't have or if the employee is a party or a witness to an investigation, says Zetter. It also reduces the risk that an employee reporting a compliance issue will be subject to retaliation, which is an OIG no-no, says van Halem.
2. **Share when legally required**. This will vary based on the law and the circumstances. **Example:** HIPAA's breach notification laws require covered entities to report to affected individuals, HHS and sometimes the media the loss of patient information. The results of some investigations may need to be reported to law enforcement.
3. **Don't leave a reporting employee out in the cold**. An effective compliance program fosters open communication and a culture where staff should feel comfortable reporting compliance concerns *(MPCA 4/5/10)*. Give an employee who wants feedback on a reported concern enough details to know how you're making a good faith response to the complaint, but you're not obligated to tell the employee everything, says Zetter.
4. **Share internally where appropriate, using proper channels,** says attorney Adrienne Dresevic, with the Health Law Partners, in Southfield, Mich. **Example:** You may need to report the results of your investigation to management, the human resources director or an employee's supervisor.
5. **Use a compliance concern or incident as a teaching tool**. While you don't want to breach confidentiality, you can use an issue in general – such as a billing error – to train staff about it. The training itself demonstrates your practice is engaged in ongoing compliance efforts, notes Zetter.
6. **If a compliance concern is a possible legal risk,** bring in an outside attorney before investigating to increase your confidentiality protection. Communications through an attorney will preserve 'attorney/client privilege,' which means it would be much harder if not impossible for the information to become public or used against you by third parties. However, this only covers you before an investigation/chart review, not after you've investigated the issue, warns Zetter.

To view the OIG's model compliance plan for physician practices, go to: *www.oig.hhs.gov/authorities/docs/physician.pdf*. *– M. Durben Hirsch*

Facebook gaffe proves costly for Rhode Island physician

Physicians are increasingly turning to social media to connect with colleagues, confer with patients and market their practices. But when your physicians breach patient confidentiality through social media, it's your practice that can run into compliance quicksand, a costly lesson recently learned by Rhode Island emergency medicine doctor Alexandra Thran, M.D. *(MPCA 5/2/11)*.

Thran posted information on her personal Facebook page about a patient she treated in the emergency department who had been in an accident. Although she did not name the patient, she posted sufficient detail about the injuries that unauthorized third parties were able to identify the patient.

Her hospital employer fired her, terminated her clinical privileges and reported the conduct to the Rhode Island Department of Health's Board of Medical Licensure and Discipline in Providence as required by law, according to Annemarie Beardsworth, the Department's Public Information Officer. The Board found Dr. Thran guilty of unprofessional conduct, fined her $500 and placed a reprimand in her permanent file. She was also ordered to attend continuing education classes about patient confidentiality.

Dr. Thran avoided more severe sanctions because she immediately deleted the patient's information when the violation was brought to her attention and worked with the board to solve the problem she created, says Beardsworth. She was unfamiliar with how Facebook worked and believed her post was private. "Each case is handled based on its own information," explains

Beardsworth. Dr. Thran now works at another Rhode Island hospital.

Social media snafus have consequences

The case highlights the significance and risk of posting patient-identifiable information on the Internet, even when it's believed the post is private. "The issue for physicians or any professional is how much of your work life you share through social media," explains attorney Julian Wright, with Robinson Bradshaw and Hinson in Charlotte, N.C.

You can end up in trouble where you don't expect it. Though Dr. Thran was punished by her employer and the state board of medicine, she could face sanctions from the Office of Civil Rights (OCR) for violating HIPAA and/or state privacy laws. She can also be sued by the patient for invasion of privacy.

This doesn't mean that you or your physicians can't post patient information, though it's clearly safest not to do so. Many physicians maintain blogs or use chat rooms to discuss cases, treatments, and other medical information. The Rhode Island Health Department doesn't have a problem with the use of social media by physicians and recognizes it's a tool to communicate with others, says Beardsworth.

The key is not to post patient-identifiable information, says Wright. "[Dr. Thran] should have been more wary regarding the details she chose to share. Either be a lot more generic or don't comment at all," he says.

Four tips for physicians to avoid privacy violations when using social media:

1. **Make sure you understand how social media works before using it**. Dr. Thran didn't realize Facebook can operate beyond the scope of one's 'friends' and that people could put together her name, place of work and posts to identify patients she had treated, especially in her small community, says Beardsworth.
2. **Don't post patient or other information that can become patient-identifiable**. Keep medical information general, says Wright.
3. **Comply with any office or practice policy on the use of social media**, says Wright. These policies vary significantly and employers have a lot of discretion regarding what they can allow and restrict.
4. **Assume every post is or will become public**. Be careful about what you post, since once it's on the internet, it will be there forever. "There should be no expectation of privacy," says Wright. If in doubt about whether the post will violate HIPAA or other privacy law, talk to your attorney or communications department first, or don't post. – *M. Durben Hirsch*

Agencies share info, nab provider for both false claims AND HIPAA violations

Be prepared for the government's compliance dragnet to get even wider. Agencies are no longer collaborating to fight provider fraud merely by sharing billing information among Medicare, Medicaid and private payers. They've begun to share unrelated information uncovered for different compliance violations, potentially exposing you to legal trouble on more than one front at once.

That's what happened to Lakewood, Wash.-based Management Services Organization Washington (MSOW), a practice management services company. The provider was under investigation by the Office of Inspector General (OIG) and Department of Justice (DOJ) for improper billing in violation of the False Claims Act when those agencies uncovered potential violations of HIPAA.

The HIPAA issue was referred to HHS, which launched its own investigation, according to Sue McAndrew, deputy director, health information privacy, HHS' Office of Civil Rights (OCR). MSOW recently entered into an integrity agreement with the OIG and settled the False Claims Act allegations for $565,000. It also signed a resolution agreement and a two-year corrective action plan with OCR, paying OCR $35,000 for the HIPAA violation.

MSOW had violated both HIPAA's privacy and security rules by impermissibly disclosing patient information for marketing without valid authorizations and failing to safeguard the information.

The upshot: It's more crucial to keep your nose clean in all areas of compliance. An investigation by one agency will no longer necessarily be "siloed." Once you're on the government's radar, your entire operation may come under scrutiny. – *M. Durben Hirsch*

HIPAA

(continued from pg. 1)

But the proposed rule adds several unexpected compliance and cost burdens on covered entities and business associates, making compliance difficult, warns attorney Kirk Nahra, with Wiley Rein in Washington, D.C.

Some of the most troublesome provisions in the proposed rule include:

1. **It creates a new right for patients to obtain an "access report."** The HITECH Act did not require this step. The access report would require you to give to the patient, within 30 days of the request, a list of all who accessed the patient's electronic health information in a "designated record set." Patients get one free access report a year. For some providers, the effective date will be Jan. 1, 2013. That means you'll need to be able to track and retrieve information, even if patients never ask for these reports, says Nahra.
2. **The rule expands what needs to be reported**. While the HITECH Act contemplated that the accounting would cover all disclosures, including those for payment, treatment and operations when an electronic health record is used, the proposed rule requires that the access report contain uses, including internal ones, as well as disclosures, so there's more for providers to report. Moreover, the proposed rule requires reporting of more than what is in the electronic health record, defining a "designated record set" as a group of records that consists of medical and billing records, employment, payment, or claims adjudication, or is used to make decisions about individuals.
3. **The rule leaves employees vulnerable**. Since the access report requires internal and external reporting of who accessed the patient's information, including the name, time and date of each access and what the user did with it, the access report will include the full name of everyone who accessed the data. That includes all employees

Take four steps to deal with the proposed accounting for disclosures rule

You may see changes to the just-released proposed HIPAA rule that expands accounting for disclosures to payment, treatment and operations *(see story, pg. 1)* when patient information is held electronically, says Phyllis Patrick, President of Phyllis A. Patrick & Associates, in Purchase, N.Y. But expect at least some components of it to be finalized. Here are four steps to take now to be prepared:

1. **Review your operations to see where you keep patient data electronically**. Even if you don't currently use an electronic health record system, you may hold information such as billing records in electronic format. Find out how much you can accomplish auditing your electronic systems and what else you may need to do to comply with this rule. "Make sure you can produce this report and pull this data, in case the access report requirement ends up in the final rule," says HIPAA consultant Frank Ruelas, in Casa Grande, Ariz. Patients also must be able to read the reports, not just raw data. Ask your vendor, regional extension center, and/or your local medical society if you need help, suggests Patrick.
2. **Use the comment period**. You have until Aug. 1 to submit comments to HHS. You can submit them electronically at *www.regulations.gov*, reference number RIN 0991-AB62 or by mail or hand delivery as noted in the rule. Make sure your professional societies are submitting comments. "I've never seen a proposed rule before that asked so much for comments regarding whether it's burdensome," says Ruelas. "If no one speaks up, it's acceptance by silence," he warns.
3. **Ask your business associates if and how they can create these access reports**, since their data will need to be included to respond to a patient's request, says Ruelas. "This is currently a weak link between doctors and business associates," he warns.
4. **Be prepared to change your Notice of Privacy Practices (NPPs)** to include the new changes once the rule becomes final, since it's a material change, says Patrick.

To view the proposed rule, go to: *www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13297.pdf*

who had legitimate reasons to access it to perform their duties, raising privacy concerns for employees, warns HIPAA consultant Frank Ruelas, in Casa Grande, Ariz. "With that, in Arizona, at least, the patient can then get copies of employees' government documents and address, and find out where you own property. You can end up with ID theft, stalkers, and lawsuits against these employees. This has serious implications," he says.

4. **The rule is ambiguous as to what data needs to be tracked**. Different phrases are used interchangeably, even though they have different meanings, says Nahra. **Example:** The rule says the access report must provide accessed information that's in the "designated record set" but also uses the phrases "designated record set information," which can be information anywhere, as well as "designated record set systems" which is not defined in the proposed rule.

5. **Most physician practices do not have the technological capability to comply**. Auditing itself isn't new to HIPAA, since the HIPAA security rule requires audit tracking, points out Phyllis Patrick, President of Phyllis A. Patrick & Associates, in Purchase, N.Y.

   The security rule allows flexibility in compliance based on a covered entity's resources and level of risk. It never required covered entities to track everything all the time, the way the proposed rule does for these electronic records and many electronic health records don't have the extensive tracking capability contemplated by the rule, warns Nahra. "HHS has a sincere belief that this isn't hard to do. I think they're wrong. No one can be compliant with this today," he says.

There is some good news. The access report, unlike the original accounting for disclosures, doesn't require that providers include the purpose of the disclosure or the address of the person disclosed to. Also, you'll only have to provide up to three years' worth of records in the access report and for accounting for disclosures. Originally, HIPAA required six years. But that's not a big deal anymore, since it's easier and cheaper to store data than it used to be, says Ruelas.

Physician practices will be especially hard hit

Compliance will be particularly hard for physician practices since, unlike hospitals, physicians often use separate medical and billing systems and outsource more to business associates, so you'll be pulling data from more than one electronic record, warns Ruelas. "There's a disconnect between what looks good on paper for an individual and how much work a [covered entity must undertake] behind the scenes," he notes.

It's also likely the creation of the right to access reports will increase requests by patients for both access reports and accounting for disclosures. "There have been hospitals that have yet to receive a request for

(continued on pg. 8)

From the
DECISIONHEALTH® PROFESSIONAL SERVICES
Case Files

Case 61: The case of the risky incident-to services

The client: A large multi-specialty group in the Northeast.

The audit: Compliance with Medicare rules for billing incident-to services.

The audit result: At least 20 of the 50 audited records raised compliance risks with Medicare's incident-to policies because documentation showed either visits for new patients or new problems – services not eligible to be billed incident-to – or the documentation did not reflect that the physician was actively involved in the patient's care.

Lessons learned:

- **Incident-to billing is used for treatment of an existing condition for an established patient under a plan of care created by the physician.** When the patient is new to the practice, or introduces a new complaint or problem during the visit, the service can no longer be billed under Medicare's incident-to rules for 100% of the payment.

Medicare services rendered by NPPs can be billed directly by enrolled NPPs for 85% of the Medicare allowable payment for the service. The patient would pay a copay of 20% of that reduced allowable charge. When a patient is new to the practice and seen by the NPP, or when the NPP treats a new complaint, the service must be billed directly if done by the NPP.

If the practice still wants to be able to bill for 100% of the allowed charge, a new patient visit must be done by the physician, who may then establish a plan of care for subsequent visits. When a new condition is introduced by the patient, the physician would need to treat the patient and establish a plan of care.

- **Even when a patient is being seen by the NPP for incident-to services, the documentation must reflect some level of ongoing involvement by the physician.** Although Medicare requirements do not specifically stipulate how often the physician has face-to-face contact with the patient or reviews the patient's records and treatments rendered by the NPP, physicians are required to provide "ongoing services of a frequency that demonstrates active involvement of the physician in the patient's care."

It's our recommendation that the physician see the patient at least once every year or once every three to four visits as a way to demonstrate ongoing physician engagement with the patient.

Sean M. Weiss, vice president & chief compliance officer of DecisionHealth can be contacted directly at *sweiss@dhprofessionalservices.com* or at 1-770-402-0855. DecisionHealth Professional Services provides full-scale medical consulting services. To learn more about our services visit us at *www.dhprofessionalservices.com* or contact us at 1-888-262-8354.

Training opportunities

- **HIPAA - Get Up to Speed, Prepare for the Next Round of Regulations and Stay Compliant** – Get details on the new burdens of the HIPAA proposed rule and fine-tune key areas of your privacy and security policies. Buy the CD at *www.decisionhealth.com/conferences/A2082*.
- **What to Do When the Auditor Knocks** – Be ready for unannounced ZPIC site visits, refute common mistakes auditors make and reduce your practice's risk of being audited. Buy the CD at *www.decisionhealth.com/conferences/A2110*.
- **Your Guide to the Elements of the Mandatory Compliance Policy Rule** – Discover how to implement a compliance program that will satisfy the OIG and protect your practice from audits and investigations. Buy the CD at *www.decisionhealth.com/conferences/A2070*.

accounting for disclosures. It's borderline ridiculous. But the floodgates could open," warns Ruelas. He's already seen television and newspaper reports on the proposed rule telling people about this new right to an access report. "A Doctor Oz, Oprah or celebrity will say something and providers will become swamped overnight," he adds.

There's also a concern that this proposed rule is setting the tone for future changes in how HHS will interpret patient rights under HIPAA.

"This may reflect some fundamental shift in HHS' philosophy," warns Nahra. – *M. Durben Hirsch*

tracker

(continued from pg. 1)

cases for either administrative actions by CMS or referral to law enforcement officials, Salters says.

"The predictive modeling (and resultant risk scores) is a screening tool that provides leads for investigation," Salters says in an email to *Medical Practice Compliance Alert*. "The risk score itself is not an adverse action that would trigger appeal rights. However, the providers will have the right to appeal any actions taken as a result of the ZPIC investigations."

"It's the same way as credit card companies would identify things that trend out of the norm," Salters says. He drew another comparison to when credit card companies identify abnormal activity on your credit card that happens in a state other than where you live.

"A provider may have access to a beneficiary I.D. and use it in an egregious fashion," Salters says. However, accidentally putting in a patient's Medicare information incorrectly will not necessarily constitute fraud, he adds. "There's a big difference between billing errors and out-and-out fraud."

The predictive analytics uses the compromised numbers database as one data source, Salters says in the email. He adds that the database consists of known or likely compromised beneficiary and provider I.D.'s. The system is based on cumulative risk scores so a provider who sees one or several comprised beneficiaries would not receive a high risk score, Salters says, but the providers who are seeing large numbers of compromised beneficiaries would receive a high risk score.

The technology typically used by credit card companies to detect fraud follows a long history of transactions and how they turn out to be fraudulent, says Thomas Goldsmith, director of communications for the Electronic Transactions Association in Washington, D.C., an international trade group representing companies who offer electronic transaction processing products and services.

Example: "If there are two uses for the same card in New York and San Francisco 15 minutes apart, we have a problem," Goldsmith says. Every transaction is transmitted back to the bank that issued the card and is also routed through the credit card company and checked for fraud, he adds.

When it comes to using similar technology to detect Medicare fraud, "I would suspect that with enough data you can associate certain patterns of data with certain types of fraud," Goldsmith says.

Active practices, other groups could be affected

The more claims you file, the greater the likelihood you'll be subject to this type of analysis, according to Wayne van Halem, president of The van Halem Group in Atlanta. Algorithms have previously been used in the post-payment process, but the new CMS technology can do more to predict and determine if a claim is false before payment, according to van Halem.

When a provider bills normally, the payer already does its data analysis but will now have access to real-time data through the new CMS initiative, van Halem says. The new technology should also put an increased focus on pre-payments, he says, and van Halem is hopeful the technology "will reduce the number of truly fraudulent claims."

The physician practice industry will join the home health and medical equipment industries in seeing an increase in pre-payment reviews as a result of the new CMS technology, according to van Halem. "It's always been 'pay and chase,' which is not very effective when fighting fraud and abuse," he says.

As the new predictive modeling technology is implemented, keep an eye out "for something that looks different and [is] causing problems for a payment of a legitimate claim," says Amy Nordeng, government affairs counsel for the Medical Group Management Association in Washington, D.C. – *C. Huntemann*

How did you get this email?

Medical Practice Compliance ALERT

June 27, 2011 | Vol. 23, Issue 12

QUICK COMPLIANCE QUIZ

HIPAA proposal and claims analyzer

HHS's proposed rule for accounting for disclosures under HIPAA goes seems to go even further than Congress did when it passed the HITECH Act in 2009. In addition, CMS is about to deploy new proprietary software to sort through claims to try and spot fraudulent actors.

Instructions: Distribute this Quick Compliance Quiz to make sure your staff understands the possible impact of the accounting for disclosures proposal and the claims tracker. **Suggested reading for staff:** *Medical Practice Compliance Alert*, June 27 issue.

1. **True or False: The proposed rule would require you to furnish to patients a list of all who accessed the patient's electronic health information.**
   - ☐ True
   - ☐ False

2. **Which of these pieces of information need to be included in accounting for disclosures reporting under the proposal?**
   - ☐ Name of each access
   - ☐ Date of each access
   - ☐ What the user did with the information
   - ☐ All of the above

3. **How many free access reports does CMS propose to allow patients to request per year?**
   - ☐ 1
   - ☐ 2
   - ☐ 3

4. **What industry did CMS base its predictive modeling for fraud detection program on?**
   - ☐ Credit card
   - ☐ Airline
   - ☐ Stock trading
   - ☐ Retail sales

5. **Where will CMS refer any findings under predictive modeling when action is required?**
   - ☐ Recovery Audit Contractor
   - ☐ Medicare Administrative Contractor
   - ☐ Zone Program Integrity Contractor
   - ☐ None of the Above

Answers

1. True

Teaching point: HHS proposes to require you to furnish to the patient, within 30 days of a request, a complete report of anyone, internal or external, who accessed the patient's electronic health information. This report, known as an access report, is proposed by HHS even though it was not part of the legislation passed by Congress mandating accounting for disclosures, known as the Health Information Technology for Electronic and Clinical Health (HITECH) Act.

2. All of the above

The access reports furnished to patients must include the name of the person or entity that accessed the information, as well as date and time the report was accessed each time. The report must also include the reason for access to the information. This includes internal and external access, raising concerns that personal information about practice employees may be required to be included.

3. 1

Teaching point: The proposed rule requires you to give the patient a free access report one time per year.

4. Credit card

Teaching point: The predictive modeling technology for health care claims is based on similar programs deployed by the credit card industry to attempt to identify and prevent fraudulent or improper transactions.

5. Zone Program Integrity Contractors

Teaching point: Any claims uncovered by the predictive modeling reviews will be shared with the Zone Program Integrity Contractors (ZPICs), Medicare contractors trained to spot and act upon fraud. The ZPICs are then tasked with deciding whether to build a case for fraud or recovery around those claims.