CCH Health Care Compliance LETTER

Volume 11, Issue 24 health.cch.com December 16, 2008

OIG: Durable medical equipment arrangement permitted

A proposed arrangement under which two companies that provide durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) would: (1) have an inventory of DMEPOS in consignment closets on-site at certain hospitals; and (2) have licensed personnel on-call or on-site at the hospitals to train and educate patients regarding certain equipment after selecting one of the companies as their supplier, did not generate prohibited remuneration under the anti-kickback statute according to the Office of Inspector General (OIG).

Arrangement details. Under the arrangement, the companies would not provide remuneration to the hospitals for use of the consignment closets. The chosen supplier would bill the patient and his or her third party payor, including Medicare or Medicaid, for the DMEPOS ordered.

The companies would ensure that personnel complied with all requirements for supplying DMEPOS, especially for suppliers of respiratory equipment. The hospitals would provide the licensed DMEPOS personnel with communication equipment to facilitate the coordination of services with the patient's treating physician, other clinicians, and the hospital's discharge planning staff, but would not charge the suppliers for the use of this equipment. The companies would also not have contact with the patients prior to the patients' selection of the supplier for respiratory equipment.

Anti-kickback statute. The anti-kickback statue makes it unlawful to knowingly and willfully to offer, pay, solicit or receive remuneration to reward referrals of items reimbursable by a federal health care program. The OIG noted in the advisory opinion that it was concerned about aggressive marketing by DMEPOS suppliers, including marketing activities that involved personal contact with beneficiaries. The activities are considered by the OIG to be highly susceptible to fraud and abuse, as they could lead to overutilization, increased costs to the federal health care program and beneficiaries, and inappropriate medical choices, as well as the adverse effects on the quality of care patients receive.

Although the proposed arrangement offered DMEPOS suppliers opportunities for access to hospital staff and patients, and was potentially susceptible to problematic marketing schemes, the OIG found that the arrangement did not violate the anti-kickback statute, because (1) there was no remuneration from the suppliers to potential referral sources, such as hospitals; (2) patients were free to choose a DMEPOS supplier; and (3) the suppliers would not provide any additional services beyond DMEPOS services. Finally, because the suppliers were only provided services in connection with DMEPOS, and not services that the hospitals were obligated to provide, there is no financial benefit to the hospitals with regard to the presence of the suppliers' personnel at their facilities. ■

OIG Advisory Opinion, No. 08-20, Nov. 26, 2008; Health Care Compliance Reporter, ¶500,200

Wolters Kluwer Law & Business

Auditing for compliance with HIPAA's minimum necessary standards

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 minimum necessary standard is flexibly written, but health information management staff must be leaders in addressing reasonable limits to help ensure privacy rights are upheld, according to experts who spoke during a recent presentation hosted by the American Health Information Management Association. One way to ensure compliance with the standard is to conduct self audits, they suggested.

Katherine Downing, director at MedPlus in Mason, Ohio, and Tony Taylor, director of health information and privacy officer at Alive Hospice in Nashville, Tennessee, advised taking a fresh look at policies and procedures, not only in the health information management (HIM) department, but also in the lab, radiology, emergency departments and nursing units. "Be your own external consultant," they recommended.

Need to know. Only individuals with a legitimate need to know may use or disclose protected health information (PHI) and each individual may only use or disclose the minimum information necessary to perform their designated role regardless of the extent of access provided to them, Downing and Taylor explained.

According to the experts, a covered entity must implement policies and procedures to identify persons or classes of persons in their workforce who need access to PHI and what category or categories of PHI is needed. For routine and recurring disclosures, they said, a facility must implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

Nonroutine disclosure. When the disclosure doesn't fit into the routine disclosure process, the facility must develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose of the request, according to Downing and Taylor. In the Privacy Rule, HHS noted that the "minimum necessary" standard is intended to reflect and be consistent with, not override, professional judgment and standards. Therefore, it's expected that covered entities will implement policies that allow people involved in treatment to have access to the entire record, as needed, they said.

Privacy officers. In addition, privacy officers must (1) identify, implement, and maintain privacy policies and procedures; (2) investigate complaints and use of sanctions; (3) perform periodic privacy risk assessments to ensure compliance; (4) ensure the delivery of privacy training to members of the workforce; and (5) monitor business associate agreements. They also must maintain current knowledge of applicable state and federal regulations as it relates to the privacy regulations and promote activities to foster privacy awareness, according to the experts.

Organization responsibilities. Covered entities should:

- Include privacy rule definitions and restrictions in employee training for health information management staff in addition to general confidentiality training. "All HIM staff are in a position that they may have to apply the minimum necessary rule at some point," Downing said.
- Conduct annual privacy refresher training using flyers, emails and presentations to keep the privacy program at the front of people's minds.
- Determine the validity of an authorization or request for PHI for an expired patient. "Just because a patient has expired does not mean their privacy and confidentiality rights go away," said Taylor.

Audit considerations. Downing and Taylor also provided a list of some things to consider when auditing HIPAA compliance:

- Are there sign-in sheets and are they used appropriately?
- Where are records stored?
- Are there computer screens that can be viewed by the public?
- Are employees signing out of computers when they leave their station?
- Are audits for minimum necessary access being done? ■

CCH Washington Bureau, Dec. 5, 2008

CCH Health Care Compliance Letter

Portfolio Managing Editor
Pamela K. Carron, J.D., LL.M

Coordinating Editors
Susan Smith, J.D., M.A.
Harold Bishop, J.D.
Anthony Nguyen, J.D.
Amber Bollman, J.D.

CCH Washington Bureau
Paula Cruickshank
DOJ, FTC–John Scorza
SEC–Peter Feltman
Health Law–Catherine Hubbard, M.A.
Tax–Jeff Carlson, Steve Cooper, Chandra Walker

Designer
Chris Tankiewicz

Requests for information about article submission and comments from readers are welcome and should be directed to Susan Smith at susan.smith@wolterskluwer.com, Tel. 847-267-2780, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Health Care Compliance Letter is published 24 times a year by CCH, a Wolters Kluwer business, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is $305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Health Care Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

Speaker offers tips for conducting effective internal investigations

When it becomes necessary to investigate possible fraud or misconduct within the workplace, it is important for the investigator to adhere to a uniform and well-documented process that is not only fair, but also creates the appearance of fairness, according to Meric Craig Bloch, vice president of corporate compliance for Adecco S.A.

"The process is more important than any single investigation," Bloch said during a teleconference sponsored by the Health Care Compliance Association. "No matter how compelling the needs of the investigation seem, don't sacrifice your standards." A fair investigation, conducted according to strict standards, ensures that findings can be defended and helps to maintain the confidence of employees.

Costs of investigation. In terms of identifying workplace problems and risk areas, business organizations may take a variety of approaches. Although some entities "are content to post a hotline number and wait until a call comes in," Bloch recommended a more proactive approach that involves using existing channels of communication within the organization's departments.

Bloch was quick to point out that although there are costs associated with conducting a workplace investigation — in terms of time, money and lost productivity within the department that is being disrupted by an investigation — there are also risks involved with not looking into possible misconduct. .

Preliminary steps. The first step in any workplace investigation, Bloch advised, should be conducting a thorough interview of the individual who reported the misconduct. The investigator should gather as much information as possible about the specifics of what occurred. "The report and the information you get from the reporter becomes your jumping-off point, and you want as firm a foundation as possible," Bloch said.

The investigator should stay alert to concerns about confidentiality and try to give the reporter a level of comfort that he or she will not face retaliation. Based on facts supplied by the reporter, the investigator can begin to assemble the story behind the misconduct report.

Whether the initial report becomes a full-blown investigation will hinge on whether the investigator finds probable cause; that is, (1) whether the investigator has a reasonable belief that misconduct occurred, and if so, (2) whether the investigator has a reasonable belief that the misconduct was committed by the persons who have been accused.

Interview process. As an investigation begins, Bloch recommends that the investigator "start outside and work in" beginning with individuals who have only a minimal connection to the wrongdoing but who often have the best vantage point from which to observe workplace culture and the dynamics between personalities.

The investigator should attempt to move forward and narrow his focus with each interview, corroborating all material facts and gathering intelligence on the individuals and events at the center of the investigation. The investigator also should evaluate the credibility of the witnesses he or she interviews. Generally, Bloch does not allow recording of interviews because of the chilling effect it can have. He also does not allow joint interviews because they encourage a "group consensus" rather than individual, independent observations and recollections.

Evaluating the evidence. The investigator should also assemble relevant documents, e-mails and other pieces of evidence. Bloch also advised the investigator to consider whether the specific incident of misconduct being investigated is the"tip of the iceberg" — a symptom of a larger, more systemic problem.

The investigator's report should focus on what did or did not occur; and should avoid the use of "adjectives, adverbs, abstract words, and editorializing," Bloch recommended. Attorney-client privilege does not protect internal investigation reports, and they are discoverable in court.

Post-investigation steps. Bloch explained that the investigation process does not end with the report. Rather, the investigator should address affected employees and departments, and even take part in the remediation process as the organization works to prevent future incidents of misconduct.

It is also good practice to contact the individual who reported the wrongdoing to inform that person that the investigation has been completed and that appropriate actions will be taken. ■

CCH Chicago Bureau, Oct. 30, 2008

Red Flag Rules: Health care providers get temporary reprieve from enforcement

by Heidi Echols, Esq., McDermott Will & Emery LLP

The Federal Trade Commission (FTC) has recently announced that it will delay enforcement of the majority of its Red Flag Rules until May 1, 2009, giving health care providers and other "creditors" time to establish appropriate identity theft prevention programs for their businesses. The FTC offered the six-month delay on enforcement to allow creditors to use "appropriate care and consideration in developing and implementing their programs." The delay also will allow the FTC "time to conduct additional education and outreach" regarding the Red Flag Rules. This article explores the requirements of the Red Flag Rules and their applicability to health care providers, and provides tips on how healthcare providers can comply with these new requirements.

On November 9, 2007, the Federal Trade Commission (FTC) and other agencies published certain final regulations that are commonly known as the Red Flag Rules.[1] "Red Flags" are patterns or activities that indicate the possible existence of identity theft. Among other things, these regulations require "creditors" that maintain certain types of accounts to develop and implement written identity theft prevention programs that are designed to detect, prevent, and mitigate identity theft in connection with such accounts.[2]

In addition, the Red Flag Rules require users of consumer reports to develop and implement reasonable policies and procedures concerning address discrepancies. Specifically, if the address from a consumer report does not match the address on file for the consumer, the user must establish a reasonable belief that the report relates to the individual about whom it requested the report.[3]

Applicability of Red Flag Rules to Health Care Providers

The Red Flag Rules were promulgated pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACTA) and apply to financial institutions and creditors. "Financial institutions" are defined under FACTA to include banks, savings and loan associations and similar entities. In the absence of highly unusual facts, health care providers would not be included in the definition of financial institutions.

The definition of a "creditor," however, is much broader. Specifically, FACTA defines a "creditor" as "any entity that regularly extends, renews, or continues credit." "Credit" is defined as the right granted by a creditor to a debtor to purchase property or services and defer payment for such purchases. These very broad definitions would seem to encompass any entity that permits a consumer to pay for services after the services are rendered. Because most health care providers typically conduct their business in this manner, the FTC believes that health care providers are covered by the definition of "creditor." [4]

Some trade associations, including the American Medical Association (AMA) and numerous other physician organizations, have expressed concern with this interpretation and have asked the FTC to address whether it is a correct interpretation to advise that physicians are creditors if they bill patients after their services are rendered.

Nonetheless, although the FTC has delayed enforcement of the majority of the Red Flag Rules, it has not indicated that it intends to change its broad interpretation of the definition of "creditor." As a result, it is prudent for health care providers to assume that if they defer payment for services, the FTC will interpret this as meeting the definition of "creditor."

In addition, many health care providers conduct other practices that would likely be considered the extension of credit. For instance, many health care providers accommodate requests for payment plans from those who are unable to make payment in full when they are billed for services. As a result, given the broad definition of "creditor," health care providers that maintain covered accounts likely will be subject to the Red Flag Rules.

Requirements of the Red Flag Rules

Identity Theft Program: The Red Flag Rules require creditors that maintain covered accounts to establish a written identity theft prevention program (the Program) containing policies and procedures that are designed to:

- identify Red Flags that are relevant to the provider's activities;
- incorporate the Red Flags into its Program;

- detect Red Flags incorporated into the Program;
- respond appropriately to Red Flags to prevent and mitigate identity theft; and
- ensure that the policies and procedures are updated periodically. [5]

The Red Flag Rules require that the initial Program be approved by the institution's Board of Directors (Board) or, if no Board exists, by a designated senior management employee. Also, the Board or senior management must be involved in the oversight and administration of the Program. The Program must provide for employee training to implement the Program effectively, and for effective oversight of any third party service provider arrangements.[6]

The mandatory compliance date was November 1, 2008, but the FTC has delayed enforcement of these requirements until May 1, 2009.[7] The FTC also has provided guidelines to consider when developing a Program.[8]

Address Discrepancies in Consumer Reports: The Red Flag Rules also include a requirement that may affect health care providers that use consumer reports, such as those that perform a credit check when scheduling elective or self-pay procedures. It requires that consumer report users develop and implement policies and procedures to handle discrepancies in the address received from the consumer reporting agency and the address on file with the user. The Red Flag Rules require users to implement procedures that allow them to form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report if there is an address discrepancy.[9]

In addition, a user must develop and implement policies and procedures for furnishing an address for the consumer that the user has reasonable confirmed is accurate to the consumer reporting agency it if has received a discrepancy in the address.[10] The mandatory compliance date for this component of the Red Flag Rules was November 1, 2008.[11] The FTC did not delay enforcement of this component of the Red Flag Rules.

Practical Tips on Implementing the Red Flag Rules

When developing and implementing an effective program to comply with the Red Flag Rules, look at practices that are in place within the organization. Health care providers already may be taking practical steps to identify potential identity theft or to detect Red Flags. In many cases, it is a matter of documenting steps that are currently performed on a regular basis and formalizing the practices. In addition, some providers have found that their HIPAA Security mitigation and incident reporting policies have been helpful in beginning the development of an identity theft program. The following may be additional helpful tips for complying with the Red Flag Rules.

Identity Theft Program

Step 1: Assemble your team. The first step in developing an effective program is to assemble a team of individuals who are empowered to act on behalf of your organization. The team should be comprised of members of the compliance office, legal, the business office, registration, scheduling and other appropriate business units and should be familiar with your operations to enable them to develop an appropriate program.

Step 2: Determine whether you maintain covered accounts. To comply with the Red Flag Rules, you will first need to determine whether you offer or maintain covered accounts. A "covered account" is defined as: (a) an account that a "creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions;" and (b) any other account that a "creditor offers or maintains for which there is a reasonably foreseeable risk to consumers or to the safety and soundness" of the creditor "from identity theft, including financial, operational, compliance, reputation, or litigation risks."[12]

The billing accounts that you maintain may meet one or both definitions of a covered account because they permit recurring transactions and balances to be paid on an ongoing basis. In addition, they often consist of sensitive information that, if breached, could put your patients at risk from identity theft. Either the patient's information used to establish the account could be compromised or you could be at risk for charges made to a fraudulently established account or to a valid account by an unauthorized party.

Step 3: Identify Red Flags for the covered accounts. You should examine the covered accounts and determine how and when products and services are delivered to the patient and charged to the covered account and what Red Flags would be relevant to the specific covered accounts. For instance, in identifying relevant Red Flags, you could consider the types of accounts you offer or maintain, the methods used to open covered accounts, methods used to access covered accounts and any prior experiences with identity theft.

The Red Flag Rules provide examples of Red Flags, but you will need to identify and incorporate into your Program Red Flags that are relevant to your activities. Red Flags could include, among others, such events as a patient who presents an identification card that appears to have been tampered with, discrepancies between admissions information and prior account information or insurance eligibility information, and suspicious personal information such as the use of a post office box rather than a physical address. Alerts, notifications or other warnings from consumer reporting agencies may be Red Flags that are appropriate for some health care providers. Other examples could be unusual patterns of activity in a covered account or notice from customers or law enforcement authorities regarding identity theft. The FTC has provided additional examples that you should review when considering which Red Flags are relevant for your business.

Step 4: Incorporate Red Flags into the Program and detect Red Flags. Once the relevant Red Flags are identified, the Program should address how Red Flags should be detected and addressed. For instance, it may be appropriate to train business office staff how to authenticate customers, monitor transactions, and verify the validity of change of address requests. The methods to detect and address Red Flags should be appropriate for the Red Flags that are identified during the assessment process.

Step 5: Respond appropriately to Red Flags to prevent and mitigate identity theft. Your policies and procedures should include appropriate responses to Red Flags that will assist in preventing identity theft. The response could include requesting additional identifying information from the patient, contacting supervisors, or security personnel to perform additional verification or monitoring accounts that show evidence of suspicious activity. In addition, you should consider factors that might increase the risk for identity theft, such as notices from consumers that they have been the victims of identity theft or security incidents in which identifying information may have been compromised. You also can look to your HIPAA Security policies and procedures to determine whether any of your incident reporting or mitigation plans could assist you in responding appropriately to Red Flags.

Step 6: Ensure that the policies and procedures are updated periodically. You should conduct a risk assessment on at least an annual basis to determine whether the Program needs to be updated to reflect changes in risks to patients or to the organization.

Step 7: Provide for effective management, oversight and implementation of the Program. To be effective and comply with the Red Flag Rules, your Board (or a senior management employee if you do not have a Board) must be involved with and provide oversight to the Program. The Board or designated employee should maintain documentation that it provided the required oversight, including minutes from Board reviews of the Program and copies of reports reviewed by the Board.

Similarly, for the Program to be effective, relevant staff members need to be trained in how to spot Red Flags and how to address them. Your training program should address the relevant components of the Red Flag Rules and you should maintain documentation of training programs and of employees who complete the training. For instance, admissions staff who check identification cards during the admission process should be trained on procedures instructing them regarding the actions to take to recognize and resolve each Red Flag relevant to them. Health care providers may be able to incorporate existing measures, such as identification procedures they implemented for HIPAA compliance or payor network participation, into their Program.

Finally, don't overlook service providers that have access to covered accounts in performing services for you. For instance, a billing company may be in a position to spot Red Flags and mitigate identity theft. You should monitor service provider behavior and require them to have appropriate programs in place, relevant to the services they provide. For instance, oversight could include requiring the service provider by contract to comply with the applicable provisions of the health care provider's Program. Or it may be appropriate for the health care provider to assess the service provider by reviewing its history of identity theft incidents or auditing the service provider's operations.

Address Discrepancies

Written policies and procedures to handle address discrepancies between consumer reporting agencies and the address on file with the user of the report could include the following:

- comparing the information in the consumer report with information that the user maintains in its own documentation or obtains from third party sources; or
- verifying the information contained in the consumer report with the consumer.[13]

These policies and procedures are fairly straight-forward and appear to be a common-sense approach to verifying addresses. You may find that you currently perform these activities.

Conclusion

The Red Flag Rules are scalable to fit health care providers' operations. The delay in enforcement should provide covered health care providers with enough time to examine their practices and develop written policies and procedures for guarding against identity theft. While there may be a cost to developing this Program, health care providers should resist a "one-size fits all" approach to identity theft mitigation and detection. The most effective programs will be the result of a risk assessment that identifies relevant and appropriate Red Flags and implements practical suggestions on how to address them. ■

Heidi Y. Echols is a partner in the law firm of McDermott Will & Emery LLP based in the firm's Chicago office. As a member of the Health Law Department, Heidi's practice focuses on information technology (IT) transactions and counseling and privacy and security issues. Heidi is chair of the firm's Health Information Technology Affinity Group and a member of the firm's e-Business Group. Heidi is also co-chair of the firm's Electronic Data Management, Privacy and Discovery Group.

Heidi has substantial experience in analysis of privacy and security issues, including the privacy and security rules promulgated under the Health Insurance Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act and the FTC's Red Flag Rules concerning identity theft. She routinely counsels clients in security breach matters, including mitigation strategies and compliance with state notification laws.

1 Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule, 72 FR 63717 (November 9, 2007).
2 16 C.F.R § 681.2.
3 16 C.F.R § 681.1.
4 *See, e.g.*, Tiffany George and Pavneet Singh, Attorneys in the FTC's Division of Privacy and Identity Protection, The 'Red Flags' Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft, Last Updated, October 30, 2008.
5 16 C.F.R § 681.2(d)(2).
6 16 C.F.R § 681.2(e).
7 72 FR 63717 at 63718.
8 16 C.F.R § 681.2(f).
9 16 C.F.R § 681.1(c).
10 16 C.F.R § 681.1(d).
11 72 FR 63717 at 63718.
12 16 C.F.R § 681.2(b)(3).
13 16 C.F.R § 681.1(c)(2) and (d)(2).

Compliance experts urge providers to create a safe environment for reporting

As the government's response to compliance violations becomes more sophisticated, the need for institutions to have an effective compliance program in place has become increasingly vital. The Health Care Compliance Association sponsored a two-part teleconference entitled "Whistleblower Claims in Healthcare," which focused on what is being done by institutions to encourage employees to report suspicious activities and enforce their compliance policies.

In recent years the government has developed more stringent efforts to address compliance issues, including the increased prosecution under the Stark law, and the expectation has arisen that institutions will be more sophisticated as a result. As such, institutions should be able to show the government that it has an effective compliance plan in place, one where there is a thorough assessment of each department of the institution on a cyclical basis, according to Linda Wawzenski, Assistant United States Attorney, Deputy Chief Civil Division, United States Attorney's Office.

Compliance professionals. Wawzenski stressed the increasing need for institutions to have professionals dedicated to compliance, especially considering that a compliance department often acts as a liaison between various departments within an institution. The presenters noted that in a situation in which the compliance officers are looked to as an authority, they are often informed of compliance risks before they become a pattern. In such cases, the institution can take steps to correct the issues internally, before they become a bigger problem that results in prosecution, Patrick Coffey, partner at Locke Lord Bissell & Liddell said.

Encouraging reporting. The presenters noted that there are a number of means to achieve an efficient compliance program for an institution and create an environment that stresses the need for employee reporting. A compliance department can provide information to employees on how to report compliance issues through the use of posters, websites, newsletters, employee handbooks and training classes, stated Terry Reeves, institutional compliance pfficer at The University of Texas Medical Branch. He stressed, however, that a good relationship with employees is vital to the effectiveness of an institution's compliance program.

Employees should know that they can report any issue, big or small, and the compliance officer will takes steps to address it. Although the compliance officer may end up dealing with many more mundane issues, an open-door policy, including a whistleblower hotline, helps to encourage reporting by fostering trust. That way, when employees become aware of a bigger issue, they feel comfortable coming to the compliance officer, Reeves said.

Organizations must develop a good relationship with employees and must be responsive to their concerns. Institutions should consider whether, "compliance is being invited to the table," Carmen Wolf, principal at BlickenWolf LLC emphasized. The presenters raised the point that there is only so much an institution can do to promote reporting, there must be action taken on the part of the board to become involved in the compliance process and take real effort to address issues that arise.

In spite of the efforts taken by the institutions and their boards to encourage employee reporting, however, they may encounter a "disconnect" between middle management and lower employees, explained Coffey. Middle management may think that they have done everything that they can do to convey to employees the ability to come forward, but when an issue arises, employees still may not feel that they can come to the manager or compliance officer, he added.

Voluntary disclosure. When issues do arise, it is important for an institution to know if and when to disclose, and if so, to whom. Although the institution's initial concern may be the monetary cost of disclosing, Wolf stressed that it is important to first determine whether, in the specific case, voluntarily disclosure is the avenue to follow. Only then should the cost to the institution be considered.

According to Wawzenski, most issues turn out to be overpayments, but that does not mean that the institution should do nothing. Should the institution owe money to the government and the compliance officer does nothing, this could amount to a crime. If the issue is an overpayment, according to Wawzenski, the institution can simply turn over the excess to the carrier or intermediary. Should the carrier suspect fraud, however, the carrier or intermediary will get the Department of Justice (DOJ) or the Office of Inspector General (OIG) involved. If the issue does not appear to be an overpayment, the institution can voluntarily disclose to the OIG.

Wawzenski finds that institutions are better off when they make a voluntary disclosure, and even more so if they are able to show the government that they have a compliance plan in operation that is it being followed, according to Wolf. Reeves cautioned that "[o]rganizations should have a plan [in place] before needing to do a voluntary disclosure."

Sources of information. Many compliance resources are available to institutions. Wawzenski suggested looking to websites of various government agencies and organizations, specifically those of the HHS, OIG, DOJ, and Taxpayers Against Fraud. Ken Blickenstaff, principal at BlickenWolf LLC, also noted that publications produced by the Healthcare Financial Management Association are valuable resources for compliance officers, and the National Association of Medicaid Fraud Control Units is an important source for information spanning more than one state. Many states and municipalities have their own False Claims Act, often identical to the federal act, of which institutions should be aware. ■

CCH Chicago Bureau, Oct. 14, 2008

Fraud & Abuse

OIG approves Wisconsin FCA, rejects New Jersey statute

As officials in Wisconsin received a letter from the Office of Inspector General (OIG) indicating that the state's false claims act meets the requirements of the Deficit Reduction Act of 2005 (DRA), New Jersey officials learned that their false claims statute will have to be amended for the state to become eligible for an increase in its share of Medicaid false claim recoveries.

The DRA provides a financial incentive for states to enact laws that establish liability for those who submit false or fraudulent claims to the state Medicaid program. States must enact statutes at least as stringent as the federal False Claims Act (FCA). If OIG concludes that a state's false claims act meets DRA requirements, the state becomes eligible for a 10-percent increase in the amount it receives as a result of any Medicaid fraud recoveries.

Qui Tam **actions.** OIG determined that New Jersey's false claims statute is not as effective in rewarding and facilitating *qui tam* actions as the FCA.

OIG concluded that the New Jersey statute falls short of the FCA because it permits the state's attorney general to take over a *qui tam* action on behalf of the state if the lawsuit is based on facts underlying a pending investigation by the attorney general. The federal FCA allows a relator to continue as a party even if an investigation was underway before the relator filed the *qui tam* action, unless the *qui tam* suit was based on a public disclosure of the allegation.

In addition, while the federal FCA provides that a relator's expenses, attorney's fees and costs should be awarded against the *qui tam* defendant, the New Jersey statute calls for those expenses to be deducted from the recovered proceeds, thereby decreasing the relator's share.

Other states. Wisconsin is the 13th state to have its false claims act approved after review by OIG. In addition to New Jersey, six other states have had their statutes rejected by OIG. ■

CCH Chicago Bureau, Dec. 1, 2008; OIG Review Letters, Nov. 4, 2008

In the News

Hospital self-reports possible health care fraud

Condell Health Network (Condell), parent corporation of Condell Medical Center, a 283-bed hospital in Libertyville, Illinois, agreed to pay $36 million to federal and state governments after voluntarily disclosing that it received improper Medicare and Medicaid payments. Condell, the largest health care provider in Lake County, Illinois, made the disclosures earlier this year while being acquired by Advocate Health Care. From 2002 through 2007, the hospital leased space in medical office buildings it owned to physicians at rental rates far below fair market value, and abated or deferred collection of rental payments for these spaces. Additionally, Condell provided loans to physicians and allowed the physicians to work off the debts at hourly rates greater than fair market value. The settlement was negotiated at a discount and Condell did not admit liability.

CCH Chicago Bureau, Dec. 1, 2008

CMS proposes NCDs for "never events"

CMS has proposed three new national coverage determinations (NCDs) related to surgical errors that are aimed at reducing the occurrence of certain serious patient care mistakes, or "never events," and preventing payment from Medicare when such events occur. The NCDs, which will be open for public comment until January 1, 2009, provide that Medicare will not cover the following three types of procedures because they are not reasonable and necessary for the treatment of a beneficiary's medical condition: (1) wrong surgical or other invasive procedure performed on a patient; (2) surgical or other invasive procedure performed on the wrong body part; and (3) surgical or other invasive procedure performed on the wrong patient. CMS may consider a procedure to fall under one of these three NCDs if it is not consistent with the correctly documented informed consent for that patient. Following the public comment period, CMS expects to issue final NCDs within 60 days.

Proposed Decision Memos and CMS Press Release, Dec. 2, 2008

Study: Medicare underpayments shift burden

Low Medicare and Medicaid reimbursements to hospitals and physicians result in increased health care costs for privately insured families, according to a new study by Milliman Inc. The study found that annual health care spending for an average family of four is $1,788 higher than it would be if Medicare and Medicaid paid the same rates as private insurers. Milliman, a Seattle-based actuarial and consulting firm, estimated that underpayments by Medicare and Medicaid annually shift approximately $88.8 billion in health care costs to private insurers. If there were no cost shift, hospital and physician costs for privately insured patients would be 15 percent lower, according to the study. The study found that cost shifting adds an estimated $1,512 to the average premium for a family of four. An estimated $1,115 of that amount is paid by the family's employer. Cost-shifting also results in an additional $276 annually in coinsurance and deductible payments, according to the study.

American Hospital Association Press Release, Dec. 9, 2008