G2 Compliance Report

For Hospitals, Laboratories and Physician Practices

Kimberly Scott, Managing Editor, kscott@G2Intelligence.com Issue 13-06 • June 2013

Inside this issue

www.G2Intelligence.com

OIG-Sanctioned Checks: All Labs Do Them, But Questions Remain

Clinical laboratories and pathology practices should pay close attention to new guidance issued by the Health and Human Services Office of Inspector General (HHS OIG) on how to handle individuals who have been excluded from federal health care programs.

On May 8, 2013, the OIG issued an updated version of a special advisory bulletin (SAB) titled "The Effect of Exclusion from Participation in Federal Health Care Programs." This updated bulletin provides new guidance on the scope and frequency of screening employees and contractors to determine whether they are "excluded individuals and entities" and answers certain other questions related to exclusions. The original bulletin, published Sept. 30, 1999 (*64 Fed. Reg. 52791*), was issued coincidental with the OIG's initiative to ensure compliance with and enforcement of exclusions.

Continued on page 2

Labs Could See Increased Scrutiny Under Proposed Incentive Reward Program

If the Centers for Medicare and Medicaid Services (CMS) has its way, changes to the Medicare Incentive Reward Program (IRP) that was created as part of the Health Insurance Portability and Accountability Act would significantly increase the number and specificity of the "tips" it receives from Medicare beneficiaries and others. Clinical laboratories and other providers should take note of these proposed changes because they represent another level of scrutiny of their activities.

As we know, the qui tam provisions of the False Claims Act (FCA) and its whistleblowers are a primary source of detecting fraud and abuse in the Medicare and Medicaid programs. These proposed changes have the effect of creating a whole new class of whistleblowers without the complexity of having to file a lawsuit and wait years for the outcome.

In a proposed rule published in the *Federal Register* April 29, 2013, CMS has proposed a change in the IRP that significantly increases the reward a person could receive for reporting instances of "sanctionable conduct" in the Medicare program. Currently, a person can receive a reward of 10 percent of the recovered amount, up to $1,000, for providing "tips" about a person or entity who has engaged in sanctionable fraud and abuse against the Medicare program that lead to the successful recovery of funds.

Continued on page 9

OIG-Sanctioned Checks: All Labs Do Them, but Questions Remain, *from page 1*

The OIG and the health care industry has now had over a decade of experience with the exclusion laws and regulations, and this updated SAB, which will supersede the September 1999 version, addresses the questions and issues that have arisen since it was published. The SAB discusses both the effects of exclusion on the excluded person or entity as well as the penalties that may be imposed on a provider that employs, arranges with, or contracts with an excluded individual or entity. It doesn't matter whether the payments are based on a cost report, fee schedule, prospective payment system, capitated rate, or any other payment methodology.

All compliance officers in any health care setting, including clinical laboratories and pathology practices, should review this updated SAB against their existing policies concerning this subject and update as needed. All training and education materials should also be updated and the auditing and monitoring programs should be updated as well.

Legal Authority and Background

The SAB includes a statutory background and a listing of the various updates that have occurred since the 1977 Medicare-Medicaid Anti-Fraud and Abuse Amendments first mandated the exclusion of physicians and other practitioners convicted of federal program-related crimes from participation in Medicare and Medicaid. It highlights some of the changes that have occurred to these regulations over time, including the 1981 enactment of the Civil Monetary Penalties Law, which authorizes HHS and the OIG to impose civil monetary penalties, assessments, and program exclusion. The OIG's sanction authority was expanded once again by the Balanced Budget Act of 1997 to include all federal health care programs. There have been other statutory amendments since the publication of the 1999 SAB that have strengthened and expanded the OIG's authority under these laws and regulations, including the Affordable Care Act (ACA) of 2010.

Determining a Person's Exclusion Status

The OIG expects all providers to, at a minimum, screen their employees and contractors against the List of Excluded Individuals and Entities (LEIE), which is maintained on the OIG Web site at *http://oig.hhs.gov*. The OIG believes that the LEIE is as accurate and provider-friendly as it possibly can be, and the Web site where the list is housed and maintained contains a variety of other information such as "Quick Tips" and a frequently asked questions section along with contact information if you have questions about the list or how to use it. Users have access to an online searchable database and a downloadable data file that is updated monthly.

***The OIG expects all providers to, at a minimum, screen their employees and contractors against the List of Excluded Individuals and Entities (LEIE), which is maintained on the OIG Web site at* http://oig.hhs.gov.**

The SAB discusses other databases that include individuals who have been excluded or debarred from participating in federal programs. The original OIG Compliance Guidance for Clinical Laboratories (*63 Fed. Reg., Aug. 24, 1998*) recommended screening against the Government Services Administration's (GSA's) Excluded Parties List System, which has been merged into the System for Award Management (SAM). SAM includes the OIG's exclusions as well as other debarment actions. Two other databases providers may use include the National Practitioner Data Bank and the Healthcare Integrity and Protection Databank. The SAB recommends that providers may use these additional resources for sanction checks but should use the LEIE as the primary database for the pur-

pose of exclusion screening for current and potential employees and contractors. As a best practice, providers should screen against the LEIE and the GSA's SAM database because that is what is recommended in the OIG compliance guidance.

The SAB recommends that providers who identify potential CMP liability because they employed or contracted with an excluded individual or entity may use the OIG's Provider Self-Disclosure Protocol to resolve the potential liability (information can be found at *http://oig.hhs.gov/compliance/self-disclosure-nto/index.asp*).

Who to Screen and How Often?

Laboratories should screen employees and contractors based on whether the item or service being provided, or the job description of the employee, includes anything that is directly or indirectly, in whole or in part, payable by a federal health care program. Current best practice is to screen all employees. If the laboratory uses temporary staff provided by an agency, either the agency or the provider may do the task, but if there is an issue, the provider is going to be held liable.

Current best practice also is to screen any individual or entity who refers any tests or other items or services paid for by a federal health care program. This screening should be performed before any claims are submitted based on an order from a physician who has not already been screened.

When it comes to contractors or vendors who provide supplies and other kinds of items and services, the laboratory may exercise some discretion. For laboratories this would include vendors who supply the instrumentation and reagents where testing is performed as well as entities involved in providing consulting services or services like billing and coding. According to the SAB, the laboratory may have some liability if they are doing business with a vendor who employs an excluded individual. Any contract with a vendor should include an obligation on the vendor's part to carry out the screening and to promptly inform the laboratory of any discrepancies it may find.

Laboratories should screen employees and contractors based on whether the item or service being provided, or the job description of the employee, includes anything that is directly or indirectly, in whole or in part, payable by a federal health care program.

Providers should screen employees and contractors prior to hiring or signing a contract. The SAB recommends monthly screening because that is how frequently the LEIE is updated, and a 2011 final regulation mandate states to screen all Medicaid-enrolled providers monthly (*76 Fed. Reg. 5862, 5897, Feb. 2, 2011*).

Consequences

There is both civil and criminal liability for an excluded individual or for an entity that employs or contracts with such an individual. Criminal liability becomes an issue when the excluded person or the employing entity knows or should have known that the exclusion existed. To avoid liability, the laboratory should ensure that a sanction check is performed on any referral source before a claim is submitted for any tests or services ordered by them.

A violation of this prohibition against submitting claims for services provided by individuals who are excluded from participation in federal programs may subject the provider to civil monetary penalties of up to $10,000 for each item or service furnished by the excluded person for which a claim is filed. The entity could also be subject to an assessment of up to three times the amount claimed and could end up being excluded itself. Further, if the provider is not taking steps to ensure these claims are not submitted, or knowingly submits claims, or deliberately ignores the requirement, it could be held criminally liable as well. Similar penalties and liabilities exist for an excluded individual. G2

Proposed Provider Enrollment Changes Could Have Effect on Labs

Proposed changes to Medicare's provider enrollment provisions could have serious consequences for laboratories that mistakenly submit an improper claim for services provided.

In a rule published in the April 29 *Federal Register*, the Centers for Medicare and Medicaid Services (CMS) proposed changes to the provider enrollment process that include not just the denial of the enrollment application but a revocation of a provider's or supplier's ability to bill the Medicare program. All currently enrolled providers could be affected by these changes.

The new provider enrollment provisions would allow denial of a provider's or supplier's enrollment if it is the current owner or was the owner of another provider or supplier that had a Medicare debt when the latter's enrollment was voluntarily or involuntarily terminated or revoked depending on certain criteria. The rule also would allow denial of enrollment or revocation of Medicare billing privileges if the provider, supplier, owner, or managing employee was convicted of a felony within the past 10 years. It would also allow revocation of Medicare billing privileges "if the provider or supplier has a pattern or practice of billing for services that do not meet Medicare requirements."

Factors That May Trigger a License Revocation

- Percentage of submitted claims that were denied
- Total number of claims denied
- Reasons for the denial
- Provider or supplier history of final adverse actions
- Length of time the pattern has continued
- How long the provider or supplier has been enrolled in Medicare

Other changes include a requirement that revoked providers and suppliers submit their remaining claims within 60 days of their revocation, limits on the ability of ambulance companies to "back bill" for services furnished prior to enrollment, and elimination of the ability of revoked providers and suppliers to submit a corrective action plan in certain circumstances.

The part of this new rule that could have significant impact on currently enrolled providers and suppliers, like clinical laboratories, is the section concerning abuse of billing privileges. Currently, a provider's or supplier's Medicare billing privileges may be revoked if it submits a claim for services that could not have been furnished to a specific individual on the date of service. The rule provides some examples, such as when the beneficiary is deceased, when the directing physician or beneficiary is not in the state or country where the services were furnished, or when the equipment necessary for testing is not present where the testing is said to have occurred.

The rule proposes to expand these revocation reasons to permit revocation if CMS determines that the provider or supplier "has a pattern or practice of billing for services that do not meet Medicare requirements, such as but not limited to, the requirement that the services be reasonable and necessary." This is different from existing revocation requirements because it addresses overall billing patterns rather than individual claims, and in these cases services were furnished but the claims do not meet Medicare requirements.

According to comments by CMS in the rule, it would "place providers and suppliers on notice that they are under a legal obligation to always submit correct and accurate claims." A laboratory or other provider can have its Medicare billing privileges revoked if it has, for instance, ineffective billing software that allows a lot of improper claims to be submitted, even if those claims are ultimately denied by Medicare for medical necessity or other reasons. CMS states, "We believe that a

Continued on page 11

G2 INTELLIGENCE

COMPLIANCE PERSPECTIVES

Managing Privacy and Security Risks: Outsourced Pathology and Laboratory Information Services

Theodore J. Kobus III, Esq.

Michael Young , Esq.

Theodore J. Kobus III is a partner and co-leader of the privacy and data protection teams at BakerHostetler in the New York office. Michael Young is an associate in BakerHostetler's Cincinnati office.

Many hospitals and medical practices outsource some or all of their pathology needs. Traditionally, such services included the provision of laboratory services up to and including around-the-clock diagnostic help by specialized teams of pathologists. More recently, vendors are now selling custom software, known as "laboratory information systems," for the management of in-house labs. These systems often handle some combination of functions, including accounting, billing, workflow management, reporting, and information storage and retrieval of lab reports. From the perspective of applicable state and federal rules, all of these arrangements pose privacy and security risks to the labs and the vendors who service them.

What Are the Information Risks?

Hackers and dishonest insiders will sometimes directly target patient or employee financial and demographic information (personally identifiable information or PII) or complete medical records with insurance information because they are useful for committing fraud or identity theft. More typically, however, thieves seek physical devices that have some independent value, such as laptops, tablets, or smart phones. Notwithstanding that the thief may not actually care about the sensitive data contained on the device, these thefts frequently result in a data security incident that must then be reported and managed.

In addition to intentional misconduct, PII and protected health information (PHI) is also at risk from negligent or inadvertent disclosure, including mishandling by outside technology vendors. Common scenarios include lost portable devices, badly secured IT systems, poor access control, or mixed-up records or reports directed to unauthorized people. Whether through intentional or unintentional misconduct, privacy or security breaches constitute events to be managed in compliance with applicable state and federal regulations and laws.

The Basics of State Law

Most state data privacy and breach notification statutes do some or all of three main things: (1) force organizations to disclose incidents involving potential identity theft and financial fraud; (2) require companies to inform consumers about their security practices; and (3) prescribe certain minimal standards for treating personal or sensitive information in light of an anti-fraud concern. State laws especially tend to focus on the disclosure of financial information or Social Security numbers (SSNs) as triggering events for an obligation to notify affected individuals and, occasionally, state attorneys general and other state regulators. Breach notification

In addition to intentional misconduct, PII and protected health information (PHI) is also at risk from negligent or inadvertent disclosure, including mishandling by outside technology vendors. Common scenarios include lost portable devices, badly secured IT systems, poor access control, or mixed-up records or reports directed to unauthorized people.

can be an expense ranging upward of six figures, only to be followed by further state investigations, fines, and private lawsuits, including class actions. Frequently, these forms of liability do not require any intentional fault or gross negligence on the part of the entity being investigated, fined, or sued.

In the medical context, it is not just the hospital, medical practice, or other traditional Health Insurance Portability and Accountability Act (HIPAA) "covered entity" that has to face the various forms of liability created by state law. Outside vendors and labs must also worry about compliance with state laws, even where the data in question is not their own. In fact, vendors in some circumstances may have an independent duty to notify a patient that a breach has occurred.

The Basics of HIPAA and the New Final Rule

In January of this year, the Department of Health and Human Services (HHS) released the long-awaited HIPAA final fule. The new final rule significantly revised privacy and security regulatory provisions affecting HIPAA-regulated entities. Outside labs and technology vendors may be accustomed to a regulatory regime in which covered entities (CEs) have all the responsibility and liability, but this arrangement changes under the new final rule with significant responsibility added to business associates (BAs). In particular, both the revised privacy and security rules contain new provisions aimed at BAs. Consequently, outside labs and technology vendors cannot escape meaningful HIPAA obligations simply by virtue of their status as BAs instead of CEs.

In the medical context, it is not just the hospital, medical practice, or other traditional Health Insurance Portability and Accountability Act "covered entity" that has to face the various forms of liability created by state law. Outside vendors and labs must also worry about compliance with state laws, even where the data in question is not their own. In fact, vendors in some circumstances may have an independent duty to notify a patient that a breach has occurred.

Notably, the final rule rejects any neat, absolute distinction between CEs and BAs, instead specifying that an organization can be both a CE and a BA. This raises regulatory compliance issues for outsourced pathology labs. From the perspective of the hiring hospital or medical practice, outsourced labs are clearly BAs, but as providers of diagnostic services with respect to individual patients, full-service pathology labs arguably also fit within the regulatory definition of *covered entity*. Because an entity may be both a BA and a CE depending on the services performed, labs in this position will be required to comply with aspects of the final rule aimed at both BAs and CEs.

There are three areas in particular that labs and technology vendors, operating as BAs, need to address under the final rule. Many of these changes can be addressed as HIPAA business associate agreements (BAAs) are updated in accordance with the final rule.

Breach Notice: The HIPAA breach-notice provisions are substantially unchanged within the new final rule. BAs are not required to notify individuals of a breach of security in the handling of PII or PHI; they are, however, required to notify the CE.

Privacy Rule: BAs may not "use or disclose" PHI except in accordance with their BA contract, and generally may not use or disclose PHI except as allowed by the rule. BAs are also restricted from the sale of PHI and from use or disclosure of genetic information for underwriting purposes. PHI must not be used or disclosed beyond the minimal amount necessary to accomplish the purpose of the use or disclosure, even where the use involves treatment, payment, and operations.

Security Rule: All BAs are now required to implement appropriate technical, administrative, and physical safeguards to secure electronic PHI. This includes protecting against "reasonably anticipated threats or hazards to the security or integrity of such information" and ensuring workforce compliance. (Thieves and hackers are probably "reasonably anticipated threats" where PII and PHI are concerned.) Lab technology vendors with cloud or software-as-a-service offerings should especially pay attention to these requirements—by accepting electronic PHI onto their own managed system, they are accepting regulatory obligations and liability that cannot be contractually avoided.

These provisions are now in effect, although the Office of Civil Rights, HHS's enforcement arm for these regulations, will not enforce compliance until Sept. 23, 2013. In general, outside pathology labs and lab vendors that already had robust privacy and security procedures in place will probably have an easier time meeting the new requirements of the final rule. Even so, given the new requirements, these service providers should review existing policies and procedures now to ensure compliance with the final rule by the September deadline. CEs should encourage their vendors to undertake such a review and should similarly undertake such a review themselves. While BAs are directly liable for their own violations of HIPAA, CEs are liable if they are not prudently managing vendors.

Security and Privacy Strategies

There is no substitute for technically strong information technology safeguards, and these basics become more important as information is dispersed more widely among vendors and outside service providers. These basics should be generally familiar.

Institutions should restrict storage and access to data; deidentify data (do not use SSNs as patient identifiers, for example); limit access rights, including within the IT group (it is bad practice, for example, to give network administration rights to every help desk technician); use strong authentication schemes (e.g., strong passwords or passphrases, no shared passwords, passwords that periodically expire, limited login attempts); have a verified, working backup system; ideally, have verified, working access to logs at the network, server, PC, and application levels; keep software patched and up-to-date, including anti-virus and malware; place appropriate restrictions on public network share drives (beware employees who inadvertently create a data privacy incident by publicly sharing files including sensitive information); manage servers appropriately (e.g., do not routinely run services under the account of a network administrator or superuser); and provide employees with a secure e-mail option.

CEs using outsourced labs should pay particular attention to mobile device security, since lab reports and other patient records are likely to be accessed from portable devices.

There are technology firms with specialized security auditing services that can help organizations test and manage these and other aspects of their IT security. Such testing could be incorporated into an annual risk assessment.

Pathology services and vendors of laboratory information systems can provide a wide range of services on many different kinds of device platforms. In these contexts, CEs and their vendors should pay attention to the amount of data that is stored on these outside systems and the period of time for which such data are available. Appropriate limits on data storage—enforced by technical controls, contractual

provisions, and/or periodic audits—are advisable. Both CEs and vendors should pay attention to access controls; for example, services that provide physicians with telephone access to lab reports should include a meaningful numeric password or other authentication procedure.

CEs using outsourced labs should pay particular attention to mobile device security, since lab reports and other patient records are likely to be accessed from portable devices. (Many pathology services treat such convenient access as a selling point.) Especially, CEs should implement strong encryption on all portable devices. Doing so can help CEs fall within a safe-harbor provision of the final rule and of many state breach-notification statutes. That, in turn, can mean avoiding regulatory fines and costly breach notice obligations in the event(uality) that a portable device is lost or stolen.

CEs should pay attention to the regulatory requirements for BAAs, including new final rule requirements. BAs must provide "satisfactory assurances" that PHI will be safeguarded, and, for these provisions, CEs should consider spelling out and requiring specific IT safeguards within the BAA. The BAA should also address the requirement to limit the use of PHI to the purposes of the contract.

Contract provisions can also be used to specify the procedures—and any indemnification and limitation on liability—for responding to a breach affecting both a vendor and vendee. Contracts should address questions like, Who controls the response to a breach? Who can be obligated to conduct a forensic investigation? What information-sharing or auditing rights does the CE have? From whom will any breach notifications come? How will external communication be controlled? What is the time frame within which a business associate must notify a covered entity of a suspected incident? Who is responsible for the costs of breach notification?

Many businesses have the mistaken impression that outsourcing services is, in itself, a good way to manage data privacy liability—and many vendors are happy to trade on this impression.

All entities should have a data breach incident response plan and an incident response team. Typically, the incident response team will consist of representatives of senior management, IT, compliance, communications, and legal. There should be clear policies and procedures within the organization for confidentially communicating a suspected data breach, and employees should receive appropriate training on these plans and policies. Entities should also consider cyber-liability insurance coverage. Even with the best practices, it is impossible to predict or prevent every event. Insurance is a good method for further addressing risks.

Conclusion

Many businesses have the mistaken impression that outsourcing services is, in itself, a good way to manage data privacy liability—and many vendors are happy to trade on this impression. But hospitals and medical practices should enter vendor arrangements with their eyes wide open: while strategic outsourcing may make sense for many reasons, legal risk avoidance is probably not one of them. With respect to breach-notice obligations, reputational risk, regulatory risk, and private lawsuits, the CE's data privacy liability substantially remains, even where services are outsourced. And, for their part, vendors increasingly share these same risks. These new realities call for careful policies and proactive management on all sides.

Theodore Kobus III can be reached at tkobus@bakerlaw.com. *Michael Young can be reached at* myoung@bakerlaw.com.

Labs Could See Increased Scrutiny, *from page 1*

Under the proposed changes, the reward amount would be increased to 15 percent of the amount recovered for the first $66 million, up to $9.9 million. The proposed rule also clarifies which individuals are eligible for a reward. Under this program, a person would have to provide specific information that leads to the recovery of funds. The proposal states, "The intent of these provisions is not to provide rewards for 'simple mistakes' or unintentional billing errors."

According to comments in the proposed rule, reporting by individuals is a proven tool for the government to detect fraud, waste, and abuse in the Medicare program. The rule points to the success of the whistleblower provisions of the FCA and the success of a similar program the Internal Revenue Service (IRS) uses to reward people who report tax fraud. It also states that while vigilant beneficiaries, caregivers, family members, and others are critical to anti-fraud efforts, many people do not report suspected fraud because they are not monitoring claims for their care or they noticed a suspicious claim but were not motivated to report it.

CMS believes that simplified Medicare Summary Notices that include instructions on how to report fraud, coupled with the increased incentives in this proposed rule, will result in more reports.

CMS believes that simplified Medicare Summary Notices that include instructions on how to report fraud, coupled with the increased incentives in this proposed rule, will result in more reports. The proposal notes that since the current IRP was put into operation in July 1998, only 18 rewards have been paid for a total of less than $16,000 and amounts collected of less than $3.5 million. In contrast, between 2007 and 2012, the IRS collected almost $1.6 billion and paid approximately $193 million in rewards. Based on this, CMS believes these changes will provide greater incentive to beneficiaries, providers, and others to report sanctionable conduct.

Who Is Eligible for a Reward

In order for an individual to be eligible to receive a reward, he or she must be the first person to report the activity and the information provided must:

- Relate to the activities of a specific individual or entity;
- Specify the time period of the alleged activities; and
- Include a degree of specificity such that a review or investigation by CMS or law enforcement would result in the imposition of a sanction.

CMS does not give a reward if the individual or entity is already the subject of review or investigation by CMS or law enforcement. The decision of whether a person is eligible to receive a reward will be at CMS's discretion.

CMS Seeking Input

CMS is seeking comments on whether it should adopt a reward structure that varies from 15 percent to 30 percent of the amounts collected rather than the flat 15 percent that is being proposed in this rule. CMS seems to prefer the 15 percent flat amount to avoid establishing a new administrative process to adjudicate the size of a reward that could range from 15 percent to 30 percent.

The proposed approach also requires the completion of an "attestation" by the reporting individual. The attestation would include a statement that the individual is not participating in the sanctionable conduct and is not otherwise ineligible to

receive a reward, that the information furnished is accurate and truthful to the best of their knowledge, and that the individual acknowledges that failing to provide truthful information could subject them to civil and criminal liability. The attestation is an attempt to discourage frivolous or irrelevant reports. CMS is seeking comments on whether it should require an attestation and if so when it should be signed and what it should contain.

CMS is also seeking comment on whether there should be an appeals process if it finds an individual is not eligible for a reward and, if so, what the appeals process should look like. The agency would also like to know whether it should consider an individual's request to waive the full refund of the reward. To be ensured consideration, comments must be received no later than 5 p.m. on June 28, 2013.

How Should Laboratories and Other Providers Respond?

First and foremost, providers should review this proposed regulation and comment on those areas they find objectionable or overly burdensome. When constructing comments, it is important to look at the rule changes themselves but also to look at the sections describing the information collection requirements and the regulatory impact analysis. If you think CMS is off on these estimates, it does not hurt to point that out to them.

This rule represents the potential creation of a new batch of whistleblowers scrutinizing the activities of health care providers, including clinical laboratories. Should this rule be finalized as it is written, providers should train their employees who interact with patients and the public about the IRP. Employees should be made to understand an innocent remark or comment to a patient, or a family member of a patient, can easily be misconstrued as evidence that improper billing or outright fraud is occurring.

Another area that should be reviewed is billing sent to patients. It is important that bills be clear and easily understandable by a patient when they include Medicare payments or denials and patient responsibility for any copays or other amounts. It should be emphasized on bills that patients who have any questions should contact the laboratory to resolve the problem. When patients do contact the laboratory, the person they are speaking to should be familiar with those aspects of the bills that your lab sends so he or she can answer questions intelligently and have the authority to resolve problems. Most important, if they tell the patient they will get back to them with an answer or a resolution, they must do so 100 percent of the time.

Proposed Provider Enrollment Changes, *from page 4*

provider or supplier should be responsible for submitting valid claims at all times and that the provider or supplier's repeated failure to do so poses a risk to the Medicare Trust Fund."

Comments by Providers and Suppliers

CMS is seeking comments on what constitutes "a pattern or practice" under these changes. The proposed rule provides a list of what might trigger an action (see chart on page 4). CMS wants to receive comments on these factors including whether additional factors should be considered and what those might be, which of the listed factors should not be considered, which of these factors should be given greater weight, if any, and finally, whether there should there be a minimum or maximum threshold established for percentage of claims denied and total number of claims denied.

CMS would also like to know if the provider and supplier community thinks that revocation is only warranted if the provider or supplier submitting the claims does so with knowledge or "reckless disregard" as to meeting Medicare requirements. CMS wants to assure the provider community that these changes are not meant to revoke billing privileges for isolated and sporadic claims denials or for innocent errors in billing. The focus is on situations where a provider or supplier regularly fails to submit accurate claims.

Summary

There are many other important aspects of this rule, and all laboratory compliance officers and billing managers should be aware of its contents. CMS is required to respond to all comments on regulations, and this is certainly a regulation that needs comment. If these regulations go through as written, a provider's or supplier's best defense is an effective and active compliance program that includes a regular system of audits and monitors of claim submittal. The emphasis on the monitors should be how many denials there are, what the denials are for, and preventive action to eliminate them to the extent possible. This is important because monitors are performed more frequently than audits, and a laboratory wouldn't want to establish a pattern or practice of submitting claims that get consistently denied because it didn't notice until its annual comprehensive billing audit.

North Carolina Lab Owner Pleads Guilty to Health Care Fraud

The former owner of Wilkesboro Clinical Laboratory faces up to 10 years in prison after pleading guilty to participating in a health care fraud scheme.

Louis Francis Curte pleaded guilty April 25 to billing Medicare for services not rendered. Curte also admitted to filing false tax returns from 2007 to 2010. In a separate civil settlement, Curte also agreed to pay $300,000 to resolve civil fraud allegations that he and his company violated the Stark law.

According to court documents, Curte owned and operated the Wilkesboro Clinical Laboratory, which from at least 2007 until about 2009 defrauded Medicare by submitting false and fraudulent claims for microbiology services that were never rendered. According to the plea agreement, the loss to Medicare was between $10,000 and $30,000.

Curte faces a maximum of 10 years in prison and a $250,000 fine for the health care fraud charges and a maximum term of three years in prison and a $250,000 fine for the tax fraud charge.

News-At-A-Glance

ABN INSTRUCTIONAL TOOL: Noridian Administrative Services has a new interactive document that serves as both instruction and tutorial for the Advanced Beneficiary Notice of Noncoverage (ABN) Form CMS-R-131. The tool will serve as an aid to assist providers and suppliers with completing the ABN form and appears to have many applications, such as training new employees in the use of the form, training physician offices, and training other users of the ABN when they are using it for laboratory services. It can also be used in remote sites, such as patient service centers, if a computer or mobile tablet device is available to handle documents in that format. The form and instructions can be found at *https://www.noridianmedicare.com/parta/train/education_center/media/abn_tutorial.html*. To use the form, simply click on an area of the form and the instructions will pop up.

2012 A RECORD FOR FALSE CLAIMS RECOVERIES: False Claims Act (FCA) cases returned over $9 billion to the government in 2012, according to Taxpayers Against Fraud (*www.taf.org*). These recoveries come from criminal fines, large state false claims act settlements, and federal settlements. According to Kristin Amerling, president of TAF, health care fraud still represents the bulk of FCA recoveries at both the state and federal level. Of the top 30 FCA cases in 2012, 19 were related to health care. What is most interesting about the statistics is the fact that all but two were initiated by whistleblowers. TAF notes that qui tam cases work well because whistleblowers bring hidden information to the government's attention and the lawyers who work with the whistleblowers act as "force multipliers." More importantly, unlike a government hotline, False Claims Act whistleblower cases must be investigated; they cannot be ignored. The government's FCA enforcement efforts in the health care arena have been directed at recovering government funds paid for services billed but not provided; services provided but not provided as billed; services provided but not billed in compliance with statutory and/or regulatory requirements or administrative guidelines; or services rendered and appropriately billed, but not provided in accordance with underlying statutory, regulatory, or contractual obligations.

G2 Compliance Report (ISSN 1524-0304) is published by G2 Intelligence, 24 Railroad Street, Keene, NH 03431-3744 USA. Tel: 800-531-1026 or +1-603-357-8101. Fax: +1-603-357-8111. Web site: www.G2Intelligence.com.

Kimberly Scott, Managing Editor, kscott@G2Intelligence.com; Heather Lancey, Designer; Beth Butler, Marketing Director; Dan Houder, COO and Publisher

Receiving duplicate issues? Have a billing question? Need to have your renewal dates coordinated? We'd be glad to help you. Call customer service at 800-531-1026.