G-2 Compliance Report

WASHINGTON G-2 REPORTS

Issue 10-04/April 2010

For Hospitals, Laboratories and Physician Practices

Labs Get New Guidance on E-Health Records

The Centers for Medicare and Medicaid Services (CMS) has issued new interpretive guidelines to help clinical laboratories align their use of health information technology, including electronic health records (EHRs), with their responsibilities under the Clinical Laboratory Improvement Amendments (CLIA).

The guidelines revise CLIA regulatory standards governing test ordering, reporting of test results, and retention of test reports. They also add a new section on managing the correction of test reports for an EHR. The guidelines were released in a March 1 memo, effective immediately, to state survey agency directors from Thomas Hamilton, director of the survey and certification group at the Centers for Medicare and Medicaid Services (CMS).

Test Request

Standard: The laboratory must have a written or electronic request for patient testing from an authorized person.

Interpretive Guidelines §493.1241(a): An "authorized person" means an individual authorized under state law to order tests or

Continued on page 2

RAC Program Will Increase Compliance Issues for Providers, Summit Speakers Say

Medicare providers could soon find themselves facing their own personal *Groundhog Day*, with a number of different contractors auditing them for the same claims cases, Richard P. Kusserow, president of Strategic Management Systems Inc., Alexandria, Va., said at the March 4 National Medicare RAC Summit, referring to a film where the main character experiences the same events over and over.

Kusserow said that as the permanent recovery audit contractor (RAC) program ramps up, providers could be audited by a RAC, which could in turn refer cases to a zone program integrity contractor (ZPIC), which could then refer the cases to the Health and Human Services Office of Inspector General.

Kusserow served as the Department of Health and Human Services inspector general from 1981 through 1992.

Continued on page 10

Kimberly Scott, Senior Editor,
kscott@ioma.com

Inside this issue

Labs Get New Guidance on E-Health Records, *from page 1*

receive test results, or both. Some states expressly authorize patients to order tests or receive (or give them access to) test results regardless of who ordered the test. In these states a laboratory may release test results directly to a patient as an "authorized person" in accordance with state law. Patients may also be considered "individuals responsible for using test results" if state law does not expressly prohibit release of test results directly to patients.

Interpretive Guidelines §493.1241(c)(1)-(c)(8): The test requisition must provide the information necessary to identify and send test results to the individual who ordered the test (the authorized person), or where applicable, to the authorized person's agent. An authorized person may also use the test requisition to designate additional individuals or entities who will be responsible for using the test results to provide care to the subject individual.

Release of Test Results

Standard: Test results must be released only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test.

Interpretive Guidelines §493.1291(f): Test results must be released to the authorized person or, if applicable, their agent. Test results must also be released to any additional individuals or entities designated on the test requisition. These entities are understood to be "responsible for using" the test results. When the authorized person and the individual responsible for using the test results receive the results, the laboratory's CLIA responsibility ends.

Transmission of Test Reports

Standard: The laboratory must have an adequate manual or electronic system(s) in place to ensure test results and other patient-specific data are accurately and reliably sent from the point of data entry (whether interfaced or entered manually) to the final report destination in a timely manner.

Interpretive Guidelines §493.1291(a): The regulations apply to manual as well as automated record systems (e.g., a laboratory information system or LIS). Regardless of the means used to transmit lab results, routine checks should be conducted to verify that transmissions are being accurately and reliably conveyed to the final report destination (the authorized person or individuals or entities responsible for using the test results).

Retention of Test Reports

Standard: The laboratory must retain or be able to retrieve a copy of the original report (including final, preliminary, and corrected reports) at least two years after the date of reporting.

Interpretive Guidelines §493.1105(a)(6): A copy, either paper or electronic, of the original report includes all information sent to the individual requesting the test or using the test results and includes the name and address of the laboratory performing the test. The copy need not be paper but may be retrieved from a computer system, microfilm, or microfiche record, as long as it contains the exact information as sent to the individual ordering the test or utilizing the test results.

The laboratory copy of the report should contain information that provides an accurate, complete, and easily understood display of previously reported

data retained or retrieved from the lab's record system. For test reports from histopathology, oral pathology, or cytology that require personnel identifiers or an authorized signature (which may be electronic), the copy must include evidence of the identifiers or signatures.

A "preliminary report" means a test result that has been reported to the authorized person, lab, or health information exchange that initially requested the test before the final test result is completed. A "partial report" means multiple tests are ordered on the same specimen or patient. If partial reports are issued for only those tests that have been completed, then the report date will be the date when all tests have been completed. However, the laboratory should be able to identify the date that each new test is appended to the report.

Correction of Test Reports

Standard: When errors are detected in test reports, the authorized person ordering the test and, if applicable, the individual using the test results should be promptly notified.

Interpretive Guidelines §493.1291(k): Errors in test results may include incorrect patient identification, test results, reference or normal ranges, interpretive information, or other significant information. Corrected reports, either hard copy or electronic, must clearly indicate both the corrected results and the fact that the report is a corrected report.

Interpretive Guidelines §493.1291(k)(1): When determining whether the laboratory gave prompt notification of test or reporting errors to the authorized person(s), their agent (if applicable), and others who are identified as responsible for using the test results on the requisition, consider where contact information was provided to the laboratory, when the error was identified, when the authorized person was notified, and the extent of the error (for example, clinically significant results reported on the wrong patient).

For the cytology standard (§493.1274), the interpretive guidelines stipulate that corrected reports should be promptly sent to the authorized person and to all known recipients of the original incorrect report.

ACLA Seeks Policy Revision on MUEs and ABNs

The American Clinical Laboratory Association (ACLA) has asked the Centers for Medicare and Medicaid Services (CMS) to revisit its position on the use of advance beneficiary notices (ABNs) for medically unlikely edit (MUE) denials. Specifically, ACLA wants CMS to make clear that ABNs are permitted when it is likely that the units of service (UOS) will exceed the allowed MUE value.

According to program transmittal 617, issued by CMS on Jan. 8, 2010, "a denial of services due to an MUE is a coding denial, not a medical necessity denial. A provider/supplier shall not issue an [ABN] in connection with services denied due to an MUE and cannot bill the beneficiary for units of service denied based on an MUE."

JoAnne Glisson, senior vice president of ACLA, says the college believes this policy is incorrect and inconsistent with the statutory and regulatory provisions relating to ABNs.

"Where a clinical laboratory knows that it is going to provide testing that

Medicare will likely deny because the UOS billed with exceed the MUE, the clinical laboratory should be permitted to obtain an ABN," writes Glisson in a Feb. 23 letter to Kimberly Brandt, director of the Program Integrity Group at CMS. "Although laboratories would prefer not to bill beneficiaries for these services, if CMS intends to enforce its MUEs, laboratories also do not believe they should be required to appeal each MUE denial or to provide such services free of charge."

Semantics

According to CMS, an MUE for a Healthcare Common Procedure Coding System (HCPCS)/Current Procedural Terminology (CPT) code is the maximum UOS under most circumstances that a provider would report for that code for a single beneficiary on a single date of service.

By virtue of the program's description, CMS has determined that UOS that exceed the MUE value are "medically unlikely," which seems virtually identical to "not medically necessary," says Glisson.

"Indeed, in our various discussions, CMS has indicated that certain MUEs, such as flow cytometry, were clinically rather than statistically based," writes Glisson in the letter. "That is, CMS has made a determination that it is seldom medically necessary to perform more than some specified UOS. As such, it is clear that CMS associates an MUE denial with a medical necessity determination. To argue that an MUE denial is anything other than a medical necessity denial seems purely semantics."

Given that an MUE denial is a determination based on whether UOS are medically reasonable and necessary, it logically follows that an ABN should be permitted so the laboratory can bill the beneficiary, argues Glisson, who requests that CMS revisit its position on the use of ABNs for MUE denials.

ACLA also has asked CMS to confirm its understanding that it is permissible for laboratories to split services into two separate line items in order to avoid triggering MUE edits when the laboratory believes that it is appropriate to bill for all of the UOS of the services billed.

MUE 'Workaround'

ACLA also has asked CMS to confirm its understanding that it is permissible for laboratories to split services into two separate line items in order to avoid triggering MUE edits when the laboratory believes that it is appropriate to bill for all of the UOS of the services billed.

According to Glisson, ACLA has been instructed to split the UOS on separate lines of a claim with the use of certain CPT modifiers in order to be reimbursed for UOS that exceed an MUE.

To the extent that claims are denied despite the use of the workaround, labs should not be required to appeal medically reasonable and necessary claims that are appropriately billed to the Medicare program, says Glisson. Permitting providers and suppliers to submit ABNs where UOS exceed MUEs is the most appropriate and logical solution, she notes.

However, in lieu of permitting ABNs, ACLA requests that CMS ensure that in using the workaround medically reasonable and necessary UOS that exceed an MUE value will not be denied and providers and suppliers will be held harmless from any potential liability that may result from following CMS's guidance to use the workaround method.

COMPLIANCE PERSPECTIVES

The HITECH Act: Is Your Organization Ready for Implementation?

Stephen R. Bentfield

Dianne J. Bourque

Karen S. Lovitch

Stephen R. Bentfield, Dianne J. Bourque, and Karen S. Lovitch are attorneys with the law firm of Mintz Levin.

While widespread adoption of interoperable electronic health records (EHRs) is still several years away, the enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) as part of the American Recovery and Reinvestment Act of 2009 (ARRA)[1] is expected to facilitate use of EHRs by ensuring their privacy and security.

To that end, the HITECH Act expanded the privacy and security requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) by (1) broadening the scope of business associates to include organizations instrumental in EHR adoption, (2) applying certain HIPAA standards previously applicable only to covered entities to business associates, (3) establishing notification requirements for security breaches involving unsecured protected health information (PHI), and (4) strengthening penalties for HIPAA violations.

Because laboratories qualify as both covered entities and business associates under HIPAA, laboratories must understand the HITECH Act and assess its impact on existing information privacy and security policies, procedures, and practices.

New Business Associate Obligations

HIPAA business associates face significant new obligations under the HITECH Act. In addition to the breach notification requirements discussed below, business associates are now subject to certain HIPAA privacy rule requirements and the entire HIPAA security rule, which previously applied only to covered entities.[2]

For the first time, HIPAA business associates are directly responsible for complying with HIPAA's implementation specifications for business associate agreements.[3] If a business associate knows that the covered entity is improperly using or disclosing PHI in violation of the business associate agreement (BAA), the business associate now must take "reasonable steps" to stop the violation.[4] An improper disclosure could occur if, for example, the covered entity repeatedly transmitted the wrong PHI to a business associate over the Internet. If the business associate cannot stop the covered entity's violation, it can terminate the BAA, or it must notify the secretary of the Department of Health and Human Services (HHS) if termination is not feasible.[5]

Although, The HITECH Act also expands the scope of business associate status to capture several types of organizations expected to be instrumental in the widespread adoption of EHRs.[6] Examples include health information exchange

[1] *See generally Title XIII of Pub. L. No. 111-5 (Feb. 17, 2009), 123 Stat. 115, 258.*
[2] *ARRA §13401(a).*
[3] *ARRA §13404.*
[4] *See 45 C.F.R. §164.504(e)(1)(ii) as modified by ARRA §13404(b).*
[5] *ARRA §§13401, 13403.*
[6] *ARRA §13408.*

organizations, regional health information organizations, e-prescribing gateways, or contract vendors that allow covered entities to offer personal health records to patients as part of EHRs.

Federal Breach Notification Requirements

Covered entities and business associates should take note of the HITECH Act's breach notification requirements because the associated administrative, financial, and reputational costs can be substantial. Before enactment, covered entities had no affirmative obligation under federal law to notify a patient if his or her PHI was lost or stolen or if the privacy and security of the PHI was otherwise compromised. However, a covered entity (and a business associate in specific instances) now must provide notification of such activity in certain circumstances.

How Is a Breach Defined?

HIPAA defines a breach as the "acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the privacy rule] which compromises the security or privacy of the protected health information" and that poses a "significant risk of financial, reputational, or other harm to the individual."[7] HHS has provided minimal guidance on how to determine whether significant risk exists. HHS has only observed that improper disclosure of a name and the fact that the person was a patient at a hospital may not pose the requisite risk under this standard of harm.[8] In contrast, if the disclosure included the type of services received (e.g., oncology treatment), the type of facility (e.g., drug and alcohol rehabilitation), or information that increased the risk of identity theft (e.g., Social Security number), then the probability is higher that significant risk could result.

There are three exceptions to the definition of "breach." A breach does not occur:

- Where an unauthorized person to whom such information was disclosed would not reasonably have the ability to retain such information;[9]
- The acquisition, access, or use of PHI by an employee acting under the authority of a covered entity or business associate was unintentional; or
- Disclosure from an individual authorized to access PHI at a covered entity or business associate to another person at the same facility was inadvertent. [10]

In these latter two instances, the PHI cannot be further used or disclosed without authorization.

When Is Notification Required?

If a breach occurs, notification is required only if it involves "unsecured" PHI. A covered entity can render PHI secure through one of two methods identified by HHS in guidance issued in April 2009.[11] First, electronic PHI is secured if it is encrypted in accordance with certain National Institute of Standards and Technology (NIST) specifications. Second, PHI, regardless of format, is secured if the media on which it is stored has been physically destroyed. Securing PHI through one of these methods allows a covered entity to avoid notifying affected individuals.

What Steps Must Be Taken When a Reportable Breach Occurs?

If a breach involves unsecured PHI, the covered entity must notify affected individuals without unreasonable delay, and in no event no more than 60 calendar days

[7] *See id.*
[8] *See Breach Notification for Unsecured Protected Health Information; Interim Final Rule, 74 Fed. Reg. 42,740, 42,745 (Aug. 24, 2009).*
[9] *ARRA §13400(1)(A).*
[10] *See ARRA §13400(1)(B).*
[11] *See 74 Fed. Reg. 19,006 (April 27, 2009).*

after discovering the breach. [12] The notice must include:

- A brief explanation of the event;
- The date of the breach and of its discovery;
- A description of the types of PHI involved;
- The steps that affected individuals should take to protect against potential harm resulting from the breach;
- A brief description of the covered entity's response, including steps to investigate and mitigate harm, and to prevent future breaches; and
- Contact procedures for follow-up questions and additional information.[13]

The method of notification varies depending upon the number of affected individuals, and the financial burden can be substantial.[14] At a minimum, written notification must be given by first-class mail to the individual's last known address or to next of kin (when applicable).[15] If a covered entity has insufficient or out of date contact information for 10 or more individuals, it also must conspicuously post notice of the breach on its Web site or in major media outlets in the affected area and maintain a toll-free breach information hot line. [16]

Breaches affecting more than 500 individuals may require two additional—and potentially costly—notification requirements. First, public notice must be provided via "prominent media outlets" of a breach affecting more than 500 residents of a state or jurisdiction.[17] Second, covered entities must notify HHS of security breaches affecting 500 or more individuals, which HHS must publish on its Web site.[18] The HHS Office of Civil Rights (OCR), which is responsible for HIPAA privacy enforcement, recently posted the initial list of breaches affecting 500 or more individuals,[19] and most of the reported breaches resulted from the theft of unsecured hard copy or electronic PHI.

Luckily, not every incident amounts to a reportable breach under HIPAA. To determine whether reporting obligations apply, a covered entity should determine the answers to the following questions:

- Has a breach involving unsecured PHI occurred?
- How many patients' PHI was accessed, acquired, or disclosed, and what were the circumstances surrounding the incident?
- Does the disclosure fit within an available exception?
- Does the breach pose a significant risk of financial or reputational harm to the individual?

---

[12] *ARRA §13402(d)(1). A breach is considered discovered by a covered entity as of the first day on which such breach was known, or by exercising reasonable diligence would have been known, to the covered entity. See ARRA §13402(c). Business associates are held to the same notification deadline as covered entities, but the relationship to the covered entity affects when the covered entity must provide notice. ARRA §13402(b), (d)(1). If a business associate is an agent, the date on which the business associate discovered the breach is imputed to the covered entity, and the notice deadline is based on the date the business associate discovered the breach. However, if the business associate is an independent contractor, then the notice deadline is based on the date the business associate notified the covered entity of the breach. See 74 Fed. Reg. at 42,754.*

[13] *ARRA §13402(f).*

[14] *A recent BusinessWeek article reported on a theft of 57 hard drives from a BlueCross BlueShield of Tennessee training center that has cost the carrier over $7 million to resolve. Robert McMillan, "Data Theft Creates Notification Nightmare for BlueCross,"* BusinessWeek, *March 2, 2010.*

[15] *ARRA §13402(e)(1)(A).*

[16] *ARRA §13402(e)(1)(B).*

[17] *ARRA §13402(e)(2).*

[18] *ARRA §13402(e)(3) and (4).*

[19] *See http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html (accessed Feb. 23, 2009).*

Do Federal and State Breach Notification Requirements Differ?

In some instances, additional steps may be necessary to comply with state data breach laws. For example, state data breach laws often apply to Social Security numbers and certain financial information maintained electronically. In contrast, HIPAA applies more broadly to PHI and does not distinguish between hard copy and electronic PHI. Similarly, state data breach laws may impose tighter deadlines or different notification procedures or may be triggered only if the breach affects a certain number of residents.

As a business associate as well as a covered entity, a laboratory should consider its reporting obligations if a breach occurs. If the laboratory was acting as a business associate, its obligation is to the covered entity, and the laboratory must comply with any notification requirements imposed by it. Absent any contractual obligations to the contrary, the covered entity must perform the risk assessment and provide notification. However, if the laboratory was acting as a covered entity, it must take all actions required by law.

Enhanced Enforcement and Penalties

The HITECH Act also expanded HIPAA enforcement powers and penalties. Covered entities therefore can expect more active HIPAA enforcement through increased civil monetary penalties (CMPs) and expanded authority for state attorneys general to bring civil HIPAA enforcement actions. HHS previously could impose CMPs ranging from $100 to $25,000 per HIPAA violation, but a covered entity now may face escalating CMPs of up to $1.5 million per calendar year.[20] The new violation categories require penalty determinations to be based on the nature and extent of the resulting harm: [21]

Violation Category	Each Violation	All Such Violations of an Identical Provision in a Calendar Year
Covered entity did not know of the violation	$100-$50,000	$1,500,000
Software Violation due to reasonable cause and not willful neglect	$1,000-$50,000	$1,500,000
Violation due to willful neglect but corrected within 30 days of discovery	$10,000-$50,000	$1,500,000
Violation due to willful neglect but not corrected within 30 days of discovery	$50,000	$1,500,000

The HITECH Act also authorized state attorneys general to bring civil actions in federal district court on behalf of residents who have been threatened or adversely affected by a HIPAA violation.[22] Under this authority, an attorney general can seek an injunction or damages of $100 per violation, not to exceed $25,000. Although these numbers may seem insignificant, related adverse publicity carries its own cost. Connecticut Attorney General Richard Blumenthal was the first to exercise this new authority in bringing suit against Health Net of Connecticut Inc. for allegedly failing to secure patient medical records and financial information involving 446,000 Connecticut enrollees.[23] This case is still pending.

---

[20] *ARRA §13410(d) (amending 42 U.S.C. §1320d-5(a)(1)).*

[21] *74 Fed. Reg. at 56,124.*

[22] *ARRA §13410(e).*

[23] *See* Connecticut v. Health Net of the Northeast, Inc., *et al, No. 3:10-00057 (D. Conn. Filed Jan. 13, 2010).*

Recommended Response to the HITECH Act's Changes

All covered entities, including laboratories, should review and revise their current business associate policies, identify all arrangements requiring a BAA, update template BAAs, and amend current BAAs. Given the increased liabilities associated with breach notification, covered entities and business associates likely will negotiate BAAs more actively than in the past, and some suggested revisions are discussed below.

BAAs should specifically address the new federal breach notification obligations and clearly establish which party bears the associated costs and responsibilities. Absent specific contract terms, the covered entity would be saddled with the entire cost and responsibility (not to mention adverse publicity) associated with a breach notification caused by a business associate. By revising BAAs to clarify which party bears the costs and responsibilities, a covered entity can equitably allocate this risk to the responsible party.

Additionally, BAAs should require business associates to report the discovery of any breach involving PHI to the covered entity promptly and to take appropriate steps to investigate and mitigate any harm. Because covered entities must give specific information to affected individuals, BAAs should require business associates to at least identify the affected individuals, describe the relevant facts and the type(s) of PHI involved, and explain the steps taken to investigate the breach and mitigate potential harm.

Finally, before contracting with a business associate, a covered entity should obtain adequate assurances that the business associate has implemented, or will implement, administrative, physical, and technical safeguards in accordance with the HIPAA security rule. Such assurances could come in the form of representations and warranties in the BAA, review of the business associate's HIPAA security policies and procedures, or both.

When acting as a business associate, a laboratory should carefully review any BAA received from another party and consider whether the laboratory functions as a business associate. For example, a laboratory should not execute a BAA received from a customer with which it no longer does business. A BAA is necessary only if one of the contracting parties is a covered entity, and the services or functions furnished by the business associate involve the use or disclosure of PHI. In addition, laboratories serving as business associates should keep track of various reporting obligations imposed by customers who are covered entities.

Conclusion

The HITECH Act and accompanying regulations are complex and far-reaching, and the potential penalties can be high for companies that fail to take appropriate steps. The HITECH Act therefore warrants careful review of existing privacy and security policies and procedures.

Stephen R. Bentfield, Dianne J. Bourque, and Karen S. Lovitch can be reached at Mintz Levin. Bentfield and Lovitch are in the firm's Washington, D.C., while Bourque is based in the firm's Boston office. Bentfield phone: 202-585-3515, e-mail: SRBentfield@mintz.com; Bourque phone: 617-348-1614, e-mail: DBourque@mintz.com; Lovitch phone: 202-434-7324, e-mail: KSLovitch@mintz.com.

RAC Program Will Increase Compliance Issues For Providers, *from page 1*

The RAC program began as a three-year demonstration, which ended in March 2008. RACs operate on a contingency-fee basis and are given the task of recovering improper Medicare payments.

The RAC demonstration was created by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 and began in 2005. The permanent RAC program will operate in all 50 states, and the full expansion is expected to be complete by the end of 2010.

Kusserow outlined several steps providers can take to handle a RAC investigation. For example, if a provider does not have internal capabilities for data analysis, it needs to have an outside entity lined up, Kusserow said. "Never has the government or contractors known more about your business than you do," Kusserow said.

He said that when providers get a demand letter from a RAC they should request to see the RAC's methodology. Once they have done this, they should seek to negotiate with the RAC. Kusserow said that while one-third of RAC appeals have been sustained in favor of providers, "you can't count on that going forward."

RAC, MAC Interaction

Karen Jackson, director, Medicare contractor management group at the Centers for Medicare and Medicaid Services (CMS), said that CMS maintains complete oversight of both RACs and ZPICs. "They're there to allow CMS to look at as many things as we think we ought to. RACs don't decide what claims to review without CMS knowing about it," Jackson said.

RACs work closely with Medicare administrative contractors (MACs), which perform claims processing for the Medicare program, Jackson said. "RACs have access to everything a MAC has paid. CMS oversight assures no overlap of analysis," Jackson said.

There are 15 MAC jurisdictions for Medicare Parts A and B claims processing, Jackson said, and nine jurisdictions are operational, Jackson said. The remaining six are in bid corrective actions, and "we hope the bid corrective actions will be completed by the end of the year," she said.

Jackson said the operational MACs have already reduced administrative costs, and the interaction between RACs and MACs can help ensure more accurate claims payments as well as a refined claims processing system.

Massachusetts Lab Settles Fraud Allegations

A Massachusetts clinical laboratory has agreed to pay $450,000 to resolve allegations that it defrauded Medicaid by improperly billing for urine drug tests, according to Attorney General Martha Coakley (D).

Life Laboratories, with facilities in the Springfield, Mass., area, allegedly improperly billed for tests that were not properly ordered by a doctor or authorized prescriber and were improperly ordered for nonmedical purposes, such as residential sobriety monitoring, a purpose not covered by Medicaid, Coakley said.

In addition, the investigation found that Life Laboratories had overcharged the state Medicaid program for urine drug and alcohol tests by failing to charge its "best price," according to Coakley.

The settlement arose from an ongoing industrywide investigation by the attorney general's Medicaid Fraud Division into urine drug tests billed by independent clinical laboratories. In 2007, the state recovered $8.15 million in a settlement with Willow Street Medical Laboratory LLC, in Lynn, and last July, Boston Clinical Laboratories Inc. settled a lawsuit filed by the attorney general in 2007 by agreeing to pay $615,000 to the state Medicaid program and $14,000 to the federal Medicare program.

Life Laboratories, an affiliate of the Sisters of Providence Health System, describes itself as a full-service medical diagnostic laboratory performing more than a million tests for health care providers at 16 locations in the Springfield area.

Strike Forces, Data Analysis Keys to Fighting Fraud

Medicare Fraud Strike Force operations have resulted in more than 270 convictions and more than $240 million in court-ordered restitutions, fines, and penalties over the past three years, Timothy J. Menke, deputy inspector general for investigations for the Department of Health and Human Services Office of Inspector General (OIG), told a March 4 hearing.

"We believe that our strike forces have had a marked sentinel effect," Menke said in his testimony before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security. "Though deterrence is difficult to quantify, we have empirical evidence that our strike force model for investigating and prosecuting health care fraud has resulted in reductions in improper claims to Medicare."

Menke said that in the first 12 months of the strike force program's existence (March 1, 2007, to Feb. 29, 2008), durable medical equipment claims in South Florida decreased by 63 percent, moving from $2.8 billion for the previous year to just under $1 billion. South Florida has had a large history of DME fraud, Menke said.

The strike force model is a joint operation between OIG and the Department of Justice and was augmented by the creation in May 2009 of the Health Care Fraud Prevention and Enforcement Action Team (HEAT) initiative. That initiative is a partnership between HHS and DOJ designed to leverage resources and expertise in the fight against fraud.

Real-Time Analysis

To expand the success of the strike force model, and improve anti-fraud efforts in general, real-time data analysis is essential, Menke said.

"To date, we have established limited access to real-time claims data but we are continuing to work to improve our access to these data, increase the number of investigators who have access, and expand access across all parts of the Medicare program," Menke said.

"In addition to having access to real-time data," he said, "it is also important that we expand our access to CMS [Centers for Medicare and Medicaid Services] systems offering advanced analysis and query tools that can be employed in mining a comprehensive national Medicare claims database."

Menke said that since implementation of the HEAT program, OIG has sent more than 130 investigators and analysts to claims database training and anticipates giving them access to a national claims database by mid-March.

The Back Page

News-At-A-Glance

PRESIDENTIAL DIRECTIVE ON FRAUD: President Obama signed a presidential memorandum March 10 directing all federal departments and agencies to expand their use of payment recapture audits to locate and recover improper payments. In announcing the move March 10, Obama said, "The health care system has billions of dollars that should go to patient care and that are lost each and every year to fraud, to abuse, to massive subsidies that line the pockets of the insurance industry. The payment recapture audit model, which already is being used by Medicare under the auspices of the recovery audit contractor (RAC) program, involves private contractors who are responsible for analyzing government payments and identifying where payments were made in error or due to fraud, waste, and abuse. The auditors receive compensation based on the amount of improper payments they are able to recover. The White House said that expanded recapture audit programs could result in at least $2 billion in recovered money over the next three years. The memorandum authorizes the director of the Office of Management and Budget to develop guidance within 90 days on steps that executive departments and agencies must take to comply with the new requirements.

HHS TO UPGRADE CLAIMS DATABASE: Officials from the Department of Health and Human Services and Department of Justice told a House panel March 4 that HHS will spend an additional $15 million to $20 million of its allocated federal funds to upgrade Medicare and Medicaid claims databases used by investigators to catch individuals committing health care fraud. Officials told the House Appropriations Subcommittee on Labor, Health and Human Services, Education, and Related Agencies that upgrading the claims databases over the next two years would help law enforcement agencies review claims as they are submitted, which would expedite the process of catching illegal activity. The Obama administration has requested a $250 million increase in discretionary funding for the Health Care Fraud and Abuse Control program (HCFAC). In fiscal 2010, HCFAC received $266 million in discretionary funding to fight health care waste, fraud, and improper payments.

G-2 Compliance Report (ISSN 1524-0304) is published by Washington G-2 Reports, 1 Washington Park, Suite 1300, Newark, NJ 07102-3130. Tel: 973-718-4700. Fax: 973-622-0595. Web site: www.g2reports.com.

Kimberly Scott, Senior Editor; Dennis Weissman, Executive Editor; Janice Prescott, Sr. Production Editor; Doug Anderson, Vice President and Publisher; Joe Bremner, President.

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 973-718-4700.