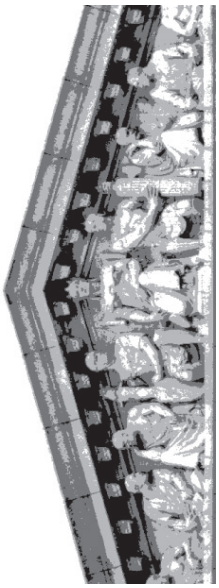

G-2 Compliance Report

WASHINGTON G-2 REPORTS

Vol. IV, No. 6, June-July 2002

For Hospitals, Laboratories and Physician Practices

HIPAA Final Rule Adopts Employer Identifier, Changes Proposed For Electronic Transactions

The Employer Identification Number (EIN) assigned by the Internal Revenue Service will become the standard unique identifier for employers in the filing and processing of electronic healthcare claims, the Centers for Medicare & Medicaid Services announced in a recent HIPAA final rule.

HIPAA (the Health Insurance Portability & Accountability Act of 1996) mandated designation of a unique identifier to help eliminate paperwork and simplify activities such as enrollment in health plans. Until now, health plans, healthcare clearinghouses and healthcare providers sometimes have used different numbers to identify the same employer when conducting business.

Healthcare providers, clearinghouses and large health plans must begin using the EIN as the standard unique identifier by July 30, 2004 (small health plans have until Aug. 1, 2005).

Electronic Transaction Revisions

CMS also announced two Notices of Proposed Rulemaking (NPRM) that would modify a number of the standards for electronic transactions adopted under a final rule published in August 2000. While the deadline for compliance with the electronic transactions rule is Oct. 16, 2002, entities that apply for an extension by this coming Oct. 15 can get up to an extra year to achieve compliance (*GCR, May '02, p. 9*).

Continued on p. 4

Tenet To Pay $56M In Triple Whammy

The nation's second largest for-profit hospital chain, Tenet Healthcare Corp. (Santa Barbara, CA) has agreed to pay $56 million to resolve fraud and false claims allegations in three separate cases.

In one case, a large group of hospitals currently or formerly operated by Tenet will pay the Federal Government and 22 states $17 million to resolve allegations that the facilities overcharged federal healthcare programs in connection with laboratory services, the Justice Department said on June 18.

Under the settlement, 139 hospitals will pay the Federal Government $16.18 million. The remaining $820,000 will go into an escrow account for the benefit of the 22 participating states.

The government alleged that the hospitals submitted claims for laboratory tests that may not have been medically necessary, properly ordered by physicians or otherwise reimbursable under certain federal healthcare programs, including Medicare, Medicaid, Tricare and the Federal Employees Health Benefits Program. The charges grew out of a nationwide probe in the mid-1990s of laboratory services provided by all U.S. hospitals. *Continued on p. 4*

Inside this issue

Physicians Urged To Get "Jump Start" On Privacy Compliance
HIPAA Expert Spells Out How To Do It

Roy Rada, MD, PhD

While most large healthcare providers are taking steps to ensure compliance with the federal rule on medical privacy slated to take effect in less than a year, many small physician practices are behind the curve on compliance preparations, according to Roy Rada, MD, PhD. The rule is part of a series of federal regulations governing electronic data exchange, as required by HIPAA (the Health Insurance Portability & Accountability Act of 1996).

"With small physician practices, there remains a surprising lack of knowledge and some indifference. Some of them still think this won't take effect," he says.

Rada, who consults on HIPAA, is president of Hypermedia Solutions Limited (Baltimore, MD) and a professor of healthcare information systems at the University of Maryland, Baltimore County.

Even though the U.S. Department of Health & Human Services in March proposed easing some of the requirements in the original privacy rule (such as eliminating the need for healthcare providers to obtain a patient's written consent before using the patient's health information for treatment, payment or healthcare operations), physician offices should not wait for those proposed changes to be finalized before implementing compliance measures to guarantee patients' privacy, Rada advises.

The good news: Developing protections is not as complicated and won't take as long as some might think. In fact, says Rada, who has developed a HIPAA guidance manual for physicians, most physician practices can develop and implement protections in less than 20 hours over eight weeks.

Initially, the practice will need to appoint a Privacy Officer; in most cases, this will be the office manager. Once the plan for assuring medical privacy is implemented, the Privacy Officer should spend a few hours each quarter reviewing forms, spot-checking medical records and ensuring that new staff have read and absorbed related training materials.

Privacy Gap Analysis

Do you have?		***Yes***	***No***
Patient Rights	Consent Form (may be optional)		
	Authorization Form		
	Notice of Privacy Practices		
	Access and Amend Policy		
	Account and Restrict Policy		
Communications Safeguards	Phone, E-mail, Fax Policy		
	Medical Record Use Guidelines		
Exceptions	Business Associate Contracts		
	Research or De-identification		
Administration	Privacy Officer		
	Tools for Documenting Behavior		
	Safeguards		
	Staff Training		

Analyze Privacy Gaps

To determine where a physician practice stands on privacy, Rada advises that the Privacy Officer start with a privacy gap analysis *(see below)*, then develop needed forms, policies and procedures.

To protect patients' rights, the Privacy Officer will need to ensure that the practice develops:

- A consent form permitting a physician to use patients' health information routinely for purposes of treatment, payment or healthcare operations.
- An authorization form for non-routine disclosure of protected health information (PHI).
- A "Notice of Privacy Practices" that describes how the physician practice is complying with applicable federal and state privacy protections.

While the consent form may be optional under final changes the government makes to the original privacy rule, Rada believes physicians should provide one nonetheless.

The Privacy Officer also should develop:

- An "access and amendment policy," stating that patients have the right to access their health information and to request that their medical records be amended (the physician may deny a request if he/she is not the originator of the information or if the information is believed to be correct).
- An "accounting and restrictions policy," stating that patients have the right to an accounting of non-routine disclosure of their PHI and the right to request additional restrictions on disclosures.

Model Employee Confidentiality Form

Security and confidentiality are a matter of concern for all persons who have access to (ENTITY) information. Each person accessing (ENTITY) data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted to him/her to preserve the security and confidentiality of this information. Therefore, all persons who are authorized to access data and resources must read and comply with (ENTITY) policy. Violators may be subject to penalties, including disciplinary action, under policies of (ENTITY) and under laws of the State of (STATE NAME). By signing this, I agree that I have read, understand and will comply with the Agreement.

_____ Signature and Date

_____ Printed Name

Communications

While the privacy rule does not require providers to establish an e-mail policy and does not specifically allow or prohibit facsimile transmission of a patient's health information, physician practices should have policies governing these types of communications to protect themselves against potential liability, Rada believes.

In fact, many states restrict faxing of certain types of health information, such as that related to AIDS, HIV or behavioral health.

The e-mail policy should specify criteria for safeguarding individually identifiable health information communicated.

Safeguards may include requirements that the information be encrypted during transmission, that a notation be made in the subject line referring to the confidential nature of the information and that the information may be distributed only to those with a legitimate "need to know." The policy also should specify criteria for e-mail retention.

A fax policy should specify what types of information may be transmitted under a cover letter that includes a confidentiality notice, warning that the faxed information is intended only for the person or entity named on the cover page.

For faxed personal health information received by the physician practice, Rada advises, the practice's Privacy Officer should designate a specific staff person to be responsible for the transmissions received on each fax machine in the office.

Exceptions

In two common situations, a physician practice may disclose PHI for non-routine use without explicit patient authorization: to business associates or for research purposes.

Rada advises physician practices to modify their contracts with business associates (lawyers, accountants, transcriptionists, etc.) to specify how the health information will be used and to require them to safeguard it appropriately.

In its proposal for changes to the original privacy rule, the government offers model language for a business associate contract. Though not mandatory, it may prove useful as an addendum to existing business associate contracts or as an aid in simplifying the contract process.

The exception related to research probably won't apply to the majority of physicians, notes Rada. But if a practice is involved in research, health records may be freely disclosed as long as they have been de-identified first. In some cases, an Institutional Review Board or a Privacy Board may approve a research proposal allowing researchers to use and disclose PHI without a patient's authorization.

Enforcing Policy

Under the privacy rule, performance must be tracked, information safeguarded and staff trained. While the rule does not specify how the tracking is to be done, Rada suggests developing computerized tables for recording disclosures.

For example, there might be one table for disclosures based on patients' authorization, business associate contracts or research; another for requests for access, amendments, accounting of disclosures and restrictions; and another listing all entities with which the physician practice has shared PHI. Common elements of these tables would include the date, to whom the information was sent, what was sent and the reason why.

A separate form should be developed to track which staff members have read the appropriate training materials.

For small offices, staff training could consist of a brief document describing the importance of protecting health information, discussing requirements of the privacy rule and spelling out office policies, Rada says.

Physicians may want to consider using an employee confidentiality form, he adds (*see above*). While not mandated by the privacy rule, this form might be used by an entity to document its ongoing effort to encourage staff to respect privacy. The signed form would be retained in the employee's personnel file.

Resource

❖ Roy Rada: 410-747-6712, *rada@hipaa-it.com*. More information is available online at *www.hipaa-it.com*.

HIPAA Final Rule, *from page 1*

One NPRM would adopt two technical implementation specifications for electronic retail pharmacy drug claims.

The other NPRM would adopt modifications to certain standards recommended by Designated Standard Maintenance Organizations, six groups selected by the Health & Human Services Secretary to maintain the standards for healthcare transactions.

The 115 modifications include 48 minor error corrections and 67 actual changes. About 20% of the changes involve requiring some data elements only in certain situations. For example, "date last seen by physician" is needed only on Medicare claims. About 40% of the changes add functionality to some transactions, such as allowing entities to cross-reference two subscribers' IDs. The rest of the changes involve either removal of certain data elements or allow certain items to be reported via external code sets rather than via data elements in the transaction. Details of the proposed modifications are available online at *http://hipaa-dsmo.org/crs/fasttrack.pdf*.

EIN Choice No Surprise

The selection of the EIN as the HIPAA unique identifier should not come as a surprise, says Gary Kieffer, a Chicago-based EDI project manager for Science Application International Corp., a research and technology company that helps providers with HIPAA compliance.

"Many providers already use the EIN; it's pretty common and most people expected that CMS would choose this as the unique identifier. This should be relatively easy to implement."

The proposed modifications to the electronic transaction rule also are unlikely to cause problems for providers, since those that file for an extension will have until Oct. 16, 2003, to make any changes that CMS ultimately finalizes, he adds. "Most people will file for the extension, so there's plenty of time to accommodate the changes."

Resources

- Gary Kieffer: 773-755-1250
- *Federal Register*, May 31, '02: Final rule on employer ID; NPRMs for electronic transactions. Online at *www.access.gpo.gov/su_docs*.

HIPAA Standards Scorecard

Final

- Electronic transactions/code sets: Promulgated August 2000. In December 2001, Congress granted an extra year to comply (to 10/16/03); requests for the one-year extension must be filed with HHS by 10/15/02. HHS proposes modifications to certain standards, 5/31/02.
- Privacy: Promulgated 12/28/00. Compliance deadline: 4/14/03 (small health plans have an additional year). Modifications proposed, 3/23/02.
- Unique identifier for employers: EIN adopted as standard, 5/31/02. Compliance deadline: 7/30/04 (small health plans, 8/1/05).

Proposed

- Security standards: Proposed 8/12/98; final version expected to be released in late summer 2002.
- Unique identifier for healthcare providers: Proposed 5/7/98.

Yet To Come

- Unique identifier for health plans
- Claims attachments

On Hold

- Unique identifier for individuals

Tenet, *from page 1*

In two unrelated cases, Tenet agreed to pay almost $39 million to settle allegations of hospital and home health fraud.

In one of these cases, a former controller charged that Brotman Medical Center (Culver City, CA) reported inaccurate square footage and number of certified beds on its hospital cost reports. Tenet acquired Brotman in 1997 and will pay $9.75 million to settle the matter. Whistleblower William Noll will receive about $1.93 million of the recovery, the Justice Department says.

In the other case, Tenet will pay $29 million to settle claims related to allocation of certain home health cost report items by Palmetto General Hospital in Florida. Palmetto's home health agency was closed in 1998. Tenet acquired Palmetto from American Medical International in 1995. Before the acquisition, the hospital repaid almost $3 million to the government for billing errors by the home health agency.

OIG Cites More Hospital Risk Areas

As it prepares to update its four-year-old hospital compliance guidance, the HHS Office of Inspector General is focusing on new potential risk areas related to implementation of Medicare's outpatient prospective payment system.

Problematic issues noted by the OIG include pass-through cost controls, outlier ambulatory payment classification (APC) payments, provider-based status, computer and information systems, advance beneficiary notices, charge description master, coinsurance collections, transitional corridor payments, multiple procedure discounting, packaging of ancillary services, observation status, readmissions, inpatient-only procedures, medical record documentation and hospital and physician coding.

The OIG invites comments from providers on these and other potential risk areas. Deadline for comments: Aug. 19. For more information, see the OIG notice in the June 18 *Federal Register* or contact Paul Johnson, 202-619-2078 or Joel Schaer, 202-619-0089.

COMPLIANCE PERSPECTIVES

CLIA Requirements: What Every Compliance Officer Needs to Know

C. Anne Pontius, MBA, CMPE, MT(ASCP), is president of Laboratory Compliance Consultants, Raleigh, North Carolina

The Corporate or Laboratory Compliance Officer (C/LCO) is responsible for identifying fraud & abuse risk areas associated with laboratory services. One such prominent area is compliance with the Clinical Laboratory Improvement Amendments of 1988 (CLIA). Since a C/LCO may or may not have technical experience in the laboratory, this article will assist those having oversight responsibilities to ensure CLIA compliance. This article does not address individual state and accreditation agency requirements.

"A Scary Voyage"

President Ronald Reagan signed the CLIA legislation into law (Public Law 100-578) on Halloween of 1988. Some took that as a clear sign it was going to be a "scary voyage" to achieve compliance. At that time, only a fraction of the estimated 150,000 clinical diagnostic labs in the U.S. had ever had federal oversight.

Rules to implement CLIA were proposed in 1990 by the U.S. Department of Health & Human Services. They caused the largest outpouring of public comments— approximately 60,000—in the history of legislation up to that point. The final rule was published in the *Federal Register* (Feb. 28, 1992), with an effective date of Sept. 1, 1992, and included many concessions requested in the comments. Since then, HHS has issued additional final rules, many updates and various technical corrections (a chronology of CLIA regulations and guidance may be viewed at *www.phppo.cdc.gov/clia/chronol.asp*).

Billing Implications

The CLIA statute has billing implications because the Omnibus Reconciliation Act of 1989 (P.L. 101-239) mandates that labs seeking payment from Medicare and Medicaid programs comply with CLIA requirements. A lab can lose its approval to bill these federal programs when principal sanctions—such as suspension, limitation or revocation of its CLIA certificate—are invoked against it. A lab that submits bills to Medicare or Medicaid for services rendered while its CLIA certificate is sanctioned is submitting potentially false claims and could be prosecuted under the federal False Claims Act.

CLIA-Defined Labs

Under the CLIA law, all facilities that perform testing for the purpose of diagnosing, preventing or treating disease or for assessing the health of human beings are subject to CLIA rules. Facilities that must comply with CLIA requirements are defined as "laboratories." The latest version of requirements can be viewed online at *www.phppo.cdc.gov/clia/regs/toc.asp*.

Laboratories (or components of a lab) that are not required to register and comply with CLIA include:

- Forensic testing facilities.
- Research labs that test human specimens but do not report the results for diagnosis, prevention or treatment of health conditions.
- Drug testing in laboratories certified by the National Institute on Drug Abuse.
- Labs under the jurisdiction of an agency of the Federal Government.

In addition, facilities that only collect and/or prepare specimens for testing or only serve as a mailing service are not considered laboratories and thus are not subject to CLIA.

Sanctioned Labs

Each year, the Centers for Medicare & Medicaid Services makes available to physicians and the general public specific information about the performance of clinical diagnostic labs (including information provided to CMS by the HHS Office of Inspector General, or OIG). A "Laboratory Registry," posted at *www.cms.gov/medicaid/clia/cliahome.htm*, lists:

(1) Labs that have been convicted under federal or state law relating to fraud & abuse, false billings or kickbacks.

(2) Labs that have had their CLIA certificate suspended, limited or revoked, and the reason(s) why.

(3) Persons who have been convicted of violating CLIA requirements, as specified in section 353(1)

of the Public Health Service Act, together with the circumstances of each case and the penalties imposed.

(4) Labs on which alternative sanctions have been imposed, showing (i) their effective date; (ii) the reason(s) for imposing them; (iii) any corrective action taken by the lab; and (iv) the verified date of compliance (if the lab has achieved compliance).

(5) Labs whose accreditation has been withdrawn or revoked and the reason(s) why.

(6) All appeals and hearing decisions.

(7) Labs against which CMS has brought suit under the CLIA rules, Section 493.1846, and the reason(s) why.

(8) Labs that have been excluded from participation in Medicare or Medicaid and the reason(s) why.

(9) Civil settlements reached with clinical labs.

(10) Corrections of any erroneous information in the previous Lab Registry.

(11) Information provided by CLIA-exempt states.

The Lab Registry lists labs by state, which makes it easy to determine those states that promote strict enforcement of CLIA sanctions. This is a good list for compliance officers to review annually to determine which enforcement actions are brought most often in their locale. This is similar to reviewing OIG notices and alerts periodically.

Test Categorizations

CLIA places all tests into one of the following test complexity categories: waived, moderate complexity or high complexity. In the moderate complexity category there is a subcategory named "provider-performed microscopy" (PPM), which is limited to a specific list of microscopy exams performed by a physician or mid-level practitioner during a patient's visit (*www.cms.gov/clia/ppmplst.asp*).

- Waived tests are considered very simple to perform and include all lab tests available by prescription or over the counter, plus more than 40 other analytes. Waived testing has minimal standards: mainly, follow the test manufacturer's instructions and permit random inspections.
- Moderate complexity tests are those that require personnel training to perform and adherence to applicable moderate complexity requirements. They comprise roughly 73% of all tests.
- High complexity tests require involvement of professionally skilled analysts to either interpret and/or perform the tests. Most tests that require subjective determinations fall in this category, such as cytology and histology.

If a lab deviates from a manufacturer's instructions for a device or procedure, the test defaults to high complexity, and the laboratory must adhere to high complexity requirements when performing it.

CLIA Requirements

CLIA regulations are divided into subparts that cover broad areas, such as Quality Control, Proficiency Testing and Quality Assurance. Most subparts specify "condition-level" requirements. Under many of these are "standards." The standards are usually detailed requirements about very specific subject matter. For example, under the Subpart "Personnel for Moderate and High Complexity Testing," there is a condition titled "Laboratories performing moderate complexity testing: laboratory director," and under that heading are two standards, "Laboratory director qualifications" and "Laboratory director responsibilities."

Labs must adhere to the requirements for the level and method of testing they perform. In other words, a lab approved for high complexity testing does not have to hold its moderate complexity testing to high complexity test requirements.

In addition to the federal CLIA rules, many states have further testing requirements. A lab is responsible for adhering to them. A lab must adhere to the most stringent requirements, either CLIA or state.

Certifications

All labs subject to CLIA regulations must register with CMS, using the CLIA application form HCFA-116 (*www.cms.gov/clia/cliaapp.asp*). A lab may request a certificate of (1) registration (issued prior to an on-site inspection), (2) waiver, (3) PPM, (4) compliance (applicable to moderate and high complexity testing) or (5) accreditation.

The only labs of those requiring oversight that are exempt from applying to CMS are those operating in states that run their own federally approved CLIA-exempt lab oversight program.

CMS determines a state's CLIA-exempt status and an accrediting organization's deemed status, based on whether their respective lab requirements are equivalent to or more stringent than the federal CLIA requirements.

The first step towards achieving CLIA compliance is to ascertain whether your lab is subject to *just* CLIA, or *just* state regulation, or CLIA *and* state regulation, or CLIA *and* accreditation organization requirements. The federal CLIA standards are considered the *minimum* platform of requirements.

CLIA Oversight

CLIA has two primary ways to exercise oversight of laboratories: inspections and proficiency testing reviews.

Inspections: Laboratories that perform moderate or high complexity testing undergo regular (routine)

inspections once every two years, either by state survey agencies with which CMS has contracted or by outside accrediting organizations which CMS has approved as CLIA accrediting bodies. For labs performing only waived or PPM tests, inspections are random. Inspections can occur in response to a complaint. Regardless of how a lab is certified, CMS retains the right to conduct an inspection as needed.

Most CLIA inspections are routine (biennial) inspections. They are either on-site or self-performed. For good performing labs—those that had zero condition-level deficiencies on their last inspection, pass proficiency testing and have not had administrative changes within the past two years—CLIA offers the self-performed AQAS or Alternate Quality Assessment Survey (CMS Form 667). This is a paper self-survey submitted to CLIA inspectors. The AQAS can only be utilized every other inspection cycle.

Proficiency Testing: This is an external quality check to ensure that a lab's methods, techniques, personnel and equipment can provide accurate, reliable test results. All labs (except waived labs) must enroll with a CMS-approved PT provider. This provider sends the lab samples it must run in the same fashion that it performs patient testing. At the time of testing, the lab is unaware of the expected result. The lab reports its PT results to the provider who grades them by comparing them with other participating labs performing the same type of test. Results are graded as pass or fail. Consistent failures can result in loss of certification to perform failed tests, along with discontinuance of Medicare payment for such tests.

Compliance measures should clearly identify when PT failures occur and the corrective actions taken to achieve accurate, reliable test results. Documentation should verify a lab director's awareness of PT failures and implementation of corrective actions.

PT requirements are the same for moderate and high complexity tests.

Quality Testing Requirements

One of CLIA's aims is to improve the quality of laboratory testing. The rules attempt to do this by requiring certain processes that promote the consistency of accurate, reliable test results. For each of the following aspects of laboratory testing—quality assurance, quality control, patient test management and personnel—the rules set specific requirements, summarized below:

Quality Assurance: These re-

CLIA Hot Spots

To ensure compliance with CLIA, the corporate or laboratory compliance officer should establish communication with the highest-level lab administrator, get on the routing list for lab compliance newsletters and stay informed about the following trouble spots:

Trouble Spot	***Recommended Action***
Change in ownership or director	Ensure changes were filed with state agency
Failed proficiency testing	Corrective action must be implemented Repeated failures may result in denied Medicare and Medicaid payments
Inspection date	Encourage zero deficiencies
Inspection report	Review most current inspection report Ensure timely reporting of corrective actions
Current CLIA certificate	Ensure it is not expired Ensure it covers the level of testing performed by the lab
Complaints	Have a mechanism to receive and address complaints from within as well as outside the lab
Cytotechnologists' overtime	Have a tracking system in place to determine the amount of time and the number of slides a cytologist reviews in a 24-hour period
Disgruntled employees	Make your presence known to all laboratory employees Give employees laminated pocket cards that list the hotline number to report CLIA violations
Terminated employees	Interview these individuals, ask if their leaving is due to having been asked to make short cuts in quality control, proficiency testing or patient testing
New or updated CLIA information	Stay plugged-in via newsletters, conferences, networking, etc.

quirements pertain to the overall operations of the laboratory and are the same for moderate and high complexity testing. This is the area that requires periodic review of policies and procedures for all facets of testing to ensure that the lab can identify non-compliance and poor quality indicators, then implement corrective measures. The QA program itself must be reviewed to ensure it is capable of identifying problems.

Quality Control: QC is more specific than QA. QC ensures that a particular reagent, method, technique, equipment or person is adequately performing at a moment in time. Each procedure has some type of QC to assure that the patient's test results are accurate. QC examples include procedures, liquids, electronic devices, maintenance or a combination of these. QC requirements differ, based on a test's complexity, specialty and/or subspecialty.

Patient Test Management: PTM primarily deals with documentation requirements for tracking specimens from their receipt in the laboratory, through the testing phases, and then to the reporting of test results. Processes need to be clearly defined so that specimens are uniquely identified at all times and the correct test results are reported for the appropriate patients. Inspectors scrutinize processes to feel comfortable that specimens will not get mixed up. There are specific requirements for the test requisition, test record and test report. PTM requirements are the same for moderate and high complexity testing.

Personnel: These requirements are comprised of qualifications and responsibilities for each CLIA-defined role. One person can fulfill as many roles for which he/she is qualified and able to uphold the specific responsibilities. The laboratory director is restricted to directing a maximum of five non-waived labs.

The specific qualifications and requirements for each role are clearly defined in the regulations:

- For a lab performing moderate complexity testing, the following CLIA roles must be filled: Clinical Consultant, Laboratory Director, Technical Consultant and Testing Analyst.
- For a lab performing high complexity testing, the CLIA-defined roles are: Clinical Consultant, Laboratory Director, Technical Supervisor, General Supervisor and Testing Analyst.

One of the top 10 deficiencies cited during CLIA inspections has to do with laboratory directors not upholding their responsibilities. Since the lab's overall operations fall squarely on the shoulders of the lab director, an inspector can easily point the finger when handing out deficiencies.

Deficiencies, Sanctions

CLIA inspectors will cite deficiencies for non-compliance with standard-level and condition-level requirements.

Deficiencies in meeting these requirements can result in sanctions, including limiting, suspending or revoking the lab's CLIA certificate. Following due process procedures, CMS can instruct Medicare to withhold payments for services it determines to be out of compliance.

Laboratories are required to respond to deficiencies with a plan of corrective action. The timeline to respond is based on the severity and level of the deficiencies cited.

For deficiencies that are not condition-level, the lab must correct them within 12 months of the inspection. For condition-level deficiencies that pose immediate jeopardy to patient health and public safety, the lab must act immediately to remove the jeopardy. If upon reinspection the lab has failed to remove the jeopardy, CMS may suspend or limit the lab's CLIA certificate no earlier than five days after the day of notice of the suspension or limitation.

CMS also may bring suit and seek a temporary injunction or restraining order against the continuance of the activity that results in immediate jeopardy to patient safety or public health.

Corrective action plans are reviewed by CLIA inspectors to determine if the steps therein are sufficient to bring the laboratory into compliance.

A lab that is found to be in compliance after implementing corrective actions is issued a CLIA certificate with a new expiration date.

A lab that submits corrective actions that are not found to achieve compliance will usually be asked to reconsider and resubmit additional corrective steps. If these still won't bring the lab into compliance, CMS may impose sanctions.

If a laboratory intentionally refers proficiency tests to an outside testing facility for the purpose of using that facility's PT results as its own, CMS is required to revoke the referring lab's CLIA certificate for at least one year and may impose civil money penalties.

Civil money penalties may be imposed for a condition-level deficiency that poses immediate jeopardy ($3,050-$10,000 per day of non-compliance or per violation) or for a condition-level deficiency that does not pose immediate jeopardy ($50-$3,000 per day of non-compliance or per violation).

Laboratories have the right to appeal CMS decisions, but sanctions stay in effect during the appeals process.

Ms. Pontius can be reached at Laboratory Compliance Consultants Inc., 4900 Waters Edge Dr., Suite 170, Raleigh, NC 27606. Tel: 919-859-3793. E-mail: CAPLCC@ aol.com.

Physician Compliance Still A Problem For Laboratories
One California Lab Tackles It Head-On, Sees Improvement

Despite guidance from the Centers for Medicare & Medicaid Services on coding requirements for diagnostic tests, a high percentage of physicians appears to be failing to provide adequate diagnostic information when submitting test requisitions.

And many labs continue to have difficulty getting the information from physicians, notes Larry Small, director of compliance and billing services for PCS Laboratory Services Group (Ann Arbor, MI).

"I see a lot of problems with anatomic pathology diagnostic coding when hospitals and pathology groups bill for technical and professional services," he tells *GCR*. "Physicians often don't provide the necessary information, and the hospital and the pathologist end up using the diagnostic findings to determine coding. In most cases, this is appropriate; however, using the clinical symptoms is often required."

Guidance From CMS

The 1997 Balanced Budget Act includes a provision requiring referring physicians to provide diagnostic information to the testing entity when they order tests. CMS elaborated on this requirement in two program memoranda within the past 10 months.

❖ PM AB-01-144 (Sept. 26, 2001) discusses how to determine the primary ICD-9-CM diagnosis code for diagnostic tests and specifies that documentation supporting the testing request must be furnished for all test orders, whether communicated via telephone, paper or e-mail. If by phone, both the treating physician and the testing facility must document the call in their respective copies of the beneficiary's medical records.

The memo also clarifies when it is appropriate for a lab to use test results to code a diagnosis. Essentially, if a specimen is abnormal, the interpreting physician or pathologist should use the findings to establish a diagnosis for coding purposes. The signs or symptoms that prompted the ordering of the test may be reported as additional diagnoses. If the specimen is normal, the interpreting physician must rely on the signs or symptoms that prompted the test request.

"If you don't have that information or it's not obvious, you have to call the doctor for the information, and therein lies the problem," Small comments. "Many laboratories don't have processes in place to contact doctors for missing information."

❖ PM AB-02-030 (Mar. 5, 2002) implements administrative changes set forth in the final rule establishing uniform lab test coverage policies, published Nov. 23, 2001. It specifies that physicians may furnish either an ICD-9-CM code or a narrative description of the diagnosis supporting the request for testing. If a lab receives a narrative description rather than an actual code, the lab may translate the narrative to the appropriate diagnosis code. The lab must maintain the documentation it receives from the physician.

Westcliff Labs Cites Progress

Westcliff Medical Laboratories in Newport Beach, CA, has found a way to improve physician compliance with diagnostic test coding requirements, though 100% compliance seems a difficult target to reach, its executives tell *GCR*.

Following passage of the 1997 Balanced Budget Act, Westcliff developed an in-house computer program that reviews test requisitions and identifies orders that may not be reimbursed by Medicare, either because they contain insufficient diagnostic or coding information or because the tests ordered are not covered by the federal program, explains Lee Ann Nichols, director of accounts receivable. Once incomplete orders are identified, lab personnel are prompted to follow up with physicians to obtain the requisite information. Westcliff also hired a client educator who visits physician offices and provides guidance on diagnostic coding requirements.

Before the program was implemented about three years ago, less than 25% of the test orders that the lab received contained appropriate diagnostic information from referring physicians, says Richard Young, a vice president and compliance officer at Westcliff. Today, about 55% of orders include the required information, he estimates.

Staff turnover in physician offices makes it difficult to achieve an even higher level of compliance, Nichols points out. "It's hard to reach 100% with the turnover we see." Another barrier to full compliance is the "lack of teeth" in the CMS guidance, she adds. "It doesn't say what will happen if the physician doesn't provide the required information. There's no hit to the pocketbook."

Resources

- ❖ Larry Small: 727-866-1311
- ❖ Lee Ann Nichols, Richard Young: 714-554-3922
- ❖ CMS Program Memos AB-01-144, AB-02-030 are available online at *www.hcfa.gov/pubforms/transmit/memos/comm_date_dsc.htm*

The "Profitable" Compliance Program
How To Maximize Productivity & Revenue

Kathleen Burke Merlo, RN

D. Douglas Miller, MD

It may be unusual to look at compliance efforts as a profit-making tool, but a billing overhaul focused on compliance can actually enable a healthcare organization to maximize both productivity and revenue, according to compliance experts at Saint Louis University School of Medicine (St. Louis, MO), which launched such an initiative in the mid-1990s.

"We did not set out to design a compliance plan that would make money," explains Kathleen Burke Merlo, MSN, RN, director of the university's compliance department. "We turned a billing process into a compliance program without adding any costs, and ultimately the billing process efficiencies netted out an increase in revenue."

Merlo and D. Douglas Miller, MD, MBA, chairman of the university's internal medicine department, discussed how to develop and benefit from a profitable compliance program during a recent audioconference held by the Health Care Compliance Association.

IMPACT'S Impact

Merlo and her colleagues began developing a compliance program for billing in 1995 by identifying lost inpatient charges through a database program called IMPACT (internal medicine patient account tracking). Each day, they received a download of data on patients admitted to the hospital the day before, and those data were automatically recorded in the internal medicine database.

Two coders were responsible for abstracting charges from charts as part of the new billing system, which initially ran concurrent with the internal medicine department's existing billing system. In the beginning, the code abstracters concentrated on inpatient evaluation & management charges and minor bedside procedures.

"One of our challenges early on was inaccurate data," says Merlo. "We ran parallel systems when we started and had our regular billing system going forward, which utilized encounter forms or superbills sent down to a central billing office. The fee abstraction process ran separately, and we immediately noticed that the number of keystroke errors was reduced. Ultimately, that impacts whether your claim gets paid or not."

Having parallel systems for a few months helped demonstrate just how effective the IMPACT system was and later helped ease the transition from the old billing system to the new one, Merlo notes. Because the new system was developed by information technology professionals on staff in the department, no new costs were incurred.

IMPACT allowed the code abstracters to enter an abbreviation or shorthand, such as CHF for congestive heart failure, and the program would automatically assign an ICD-9-CM diagnosis code from a data file downloaded from the American Medical Association. Eventually, the university stripped out codes that were never used. Project managers also developed a special internal "unbillable" CPT code, which helped the department track services that were provided but could not be billed.

"We were also able to use those unbillable codes to educate our faculty and physicians about what they were doing," essentially improving their compliance with documentation and billing rules.

At the same time, Merlo's project team relied on physicians to help educate the code abstracters about different diagnoses and treatments, which helped in determining appropriate codes. "We had a very positive relationship between the fee abstractionists and the physicians," she recalls.

Revenue, Productivity Gains

The new fee abstraction system allowed the internal medicine department to decrease billing and charge-entry personnel by half and to bypass the central billing office—which had contributed to delays in processing claims, according to Merlo.

Abstracting Charges From Patient Charts
Key Benefits Of The Billing Initiative

1. Decrease audit liability
2. Improve the accuracy of CPT and ICD-9-CM coding
3. Provide efficient means of handling changes
4. Increase accuracy of data entry
5. Ensure that professional charges are billed and paid correctly
7. Reduce lag days (Saint Louis University reduced the lag time from 146 days to 14 within two months of implementing the new billing compliance system)
8. Improve ability to self-regulate and enforce sanctions

"The central billing office contributed to the number of lag days. By eliminating their involvement, we were able to reduce lag days significantly, which in turn improved cash flow."

Improved accuracy of the claims also helped save money by reducing the number of times a claim was "kicked back" for additional information. Capturing the data more accurately the first time saved the department $5-$15 per claim, Merlo estimates.

"We ended up with what was essentially a 'free' compliance process. We developed a billing process that completely integrated all our billing compliance principles and goals. In the first year alone, the department of internal medicine increased revenue by $1.5 million."

Perhaps the greatest savings came from high-revenue divisions where complex procedures are performed, adds D. Douglas Miller. Not only did staff do a better job of capturing services, but they also were able to code legitimately at a higher level for several complex services that had been undercoded in the past. The two divisions with the highest unbillable rates in 1997-98—gastroenterology and cardiology—reduced their unbillable service rates in 1998-99 by more than 7%.

Factors For Success

The success of the billing compliance program developed by the Saint Louis University Department of Internal Medicine hinged on four factors, according to Miller:

1. A detailed monthly activity tracking system.
2. Continuing education of key department managers.
3. Continuing education of individual physicians.
4. Institutional commitment at the highest levels.

The project leaders involved the corporate compliance office early in the planning process and convinced physicians to buy into the program through personal letters and one-on-one training sessions, Miller says. Regular feedback and data reporting helped keep physicians involved in the process.

"Management accountability is also important. I meet with our departmental compliance officer on a regular basis, and we also work closely with the compliance team at the institutional level."

The project team set realistic "stretch" goals that allowed the new program to grow and improve, he says. "As you enter into the program, you want to make sure that people understand what the target is and where you want to be at the end of the year."

Resources

- Kathleen Burke Merlo: 314-268-5545
- D. Douglas Miller: 314-577-8760

For the Record

Claims Review: New OIG Guidelines

The HHS Office of Inspector General has modified its claims review guidance for healthcare providers operating under corporate integrity agreements (CIAs). Though not expressly required by all CIAs, the OIG suggests that reviews of claims that are conducted by an independent review organization (IRO) or by a provider (with verification by an IRO) be performed in accord with the following guidelines.

A discovery sample of at least 50 randomly selected units, or claims, should be examined. For each claim examined, the reviewer should determine the dollar difference between the provider's actual reimbursement and the amount the provider should have been reimbursed.

Once all sampling units have been reviewed, the results of each are added together (underpayments may be netted or offset from overpayments). The resulting calculation is the net overpayment. The review divides the net overpayment by the total dollar amount of the sample. The resulting calculation is the net financial error rate.

If the net financial error rate equals or exceeds 5%, the reviewer should examine a full sample. The OIG recommends that a full sample include enough claims to estimate the overpayment in the population within a 90% confidence and 25% precision level. The reviewer may use the discovery sample as a part of the full sample, if statistically appropriate.

If a full sample is examined, the OIG also recommends that a provider conduct a systems review. Specifically, for each claim that resulted in an overpayment, the reviewer should perform a "walk through" of the system(s) and process(es) that generated the sample to identify any problems or weaknesses.

Additional information on the new OIG guidance, along with a list of frequently asked questions on claims review, is available online at *http://oig.gov/fraud/cia/docs/ciafaq1.html#5.*

The Back Page

News-At-A-Glance

Stark Payout: Marycrest Health System (Minot, ND) and 13 other defendants have agreed to a $5 million settlement of a Colorado whistleblower case over allegations that the facility filed false claims to Medicare and Medicaid and violated the Stark physician self-referral law. The agreement settles a case filed against UniMed Medical Center by former president and CEO Gary Kenner. Marycrest is the former owner of UniMed. Kenner alleged that UniMed entered into financial ties with Medical Arts Clinic, a physician group in Minot, to induce the physicians to refer patients for hospitalization.

Bankrupt Hospital Sued: The U.S. Attorney for the Northern District of Illinois has filed a civil lawsuit against the CEO of the now-shuttered Edgewater Hospital and Medical Center in Chicago and the firms that managed the hospital, alleging that the defendants defrauded Medicare and Medicaid in excess of $18 million between 1995 and 2000. The suit seeks three times the actual amount of the fraud as damages, and other monetary penalties. Named as defendants: Peter Rogan of Valparaiso, IN; Braddock Management LP, Bainbridge Management LP and Bainbridge Management Inc. The defendants are charged, in part, with providing kickbacks; performing (or causing others to perform) unnecessary medical procedures, including blood tests; and falsifying records.

Former Damon VP Sentenced: William Thurston, a former senior vice president of now-defunct Damon Clinical Laboratories (Needham, MA), was sentenced on June 26 to three month's imprisonment, followed by three years of supervised release, for conspiring to defraud Medicare of millions of dollars. He was convicted last Dec. 17 of conspiring to deceive physicians into ordering an unnecessary blood test, ferritin, by bundling it into a commonly ordered automated chemistry profile. In October 1996, the Damon Corp. pled guilty to conspiracy for the same conduct as well as other misconduct and paid $119 million to the government.

Experimental Device Settlement: Seven hospitals will pay more than $6.3 million to settle false claim allegations that between 1987-94 they unlawfully charged federal healthcare programs for surgical procedures using experimental cardiac devices.

Hospitals participating in the settlement and the amounts involved are: Scripps Memorial Hospital (La Jolla, CA) and Scripps Green Hospital (San Diego), $3.8 million; Presbyterian Hospital and Shadyside Hospital (Pittsburgh, PA), $1.5 million; Oklahoma City's INTEGRIS Baptist Medical Center, $629,000; Hoag Hospital (Newport Beach, CA), $305,000; and St. Joseph's Regional Medical Center (South Bend, IN), $107,000.

Another PATH Settlement: Howard University Hospital (Washington, DC) has agreed to pay $1.8 million to resolve civil claims arising from the government's initiative called PATH (Physicians at Teaching Hospitals). The university conducted a self-audit which found a lack of documentation that Medicare requires to establish that faculty physicians personally provided services to patients. It also found that for other services, claims had been submitted that didn't comply with rules for calculating payment for physician services. No evidence was found of improper medical care.

G-2 Compliance Report (ISSN 1524-0304). © 2002 Washington G-2 Reports, 1111 14th St, NW, Suite 500, Washington DC 20005-5663.

Tel: (202) 789-1034. Fax: (202) 289-4062. Order Line: (212) 629-3679. Website: www.g2reports.com.