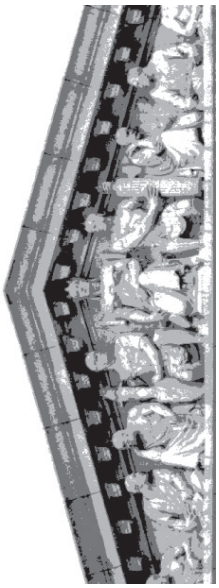


G-2 Compliance Report

WASHINGTON G-2 REPORTS

Vol. V, No. 8, September 2003

For Hospitals, Laboratories and Physician Practices

Get Ready For Medicare Coding Changes For Labs

New Policy, Revised Codes Take Effect Oct. 1

Independent and hospital labs have only about a month left before they must implement several changes affecting coding of lab claims, including a new requirement that all Medicare Part B claims contain valid ICD-9 codes.

Effective Oct. 1, 2003, all Part B laboratory claims must contain a valid ICD-9 code or they will be returned to the provider as "unprocessable," according to the Centers for Medicare & Medicaid Services. The new requirement is detailed in several recent program memos—B-03-045, B-03-046 and AB-03-091. ICD-9 code changes for 2004 are also listed in AB-03-091. While these code changes take effect Oct. 1, both the old and new codes will be accepted until January 2004, says CMS.

Also on Oct. 1, changes to the national coverage determination (NCD) edit software go into effect, as described in transmittal AB-03-104. Again, both old and new codes will be accepted through the end of the year. Among just a few of the changes:

- Diagnosis code 401.1, benign essential hypertension, is added to the list of ICD-9 codes for lipid testing.
- In the serum iron studies NCD list of covered diagnoses, code 282.4 is replaced with

➥ *p. 2*

Inside this issue

Medicare Reform May Bring Needed Changes

Healthcare providers are likely to see some welcome changes to the Medicare regulatory process if and when Congress approves a final Medicare reform bill, possibly this fall.

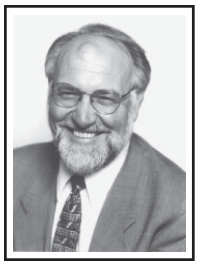
House and Senate conferees who have been working on hammering out differences between two versions of Medicare reform legislation have already reportedly reached agreement on regulatory and contracting reform provisions, which they say will help streamline complexities in the Medicare program and allow providers to focus on patient care, rather than excessive paperwork.

In general, the agreement aims to modernize the contracting system, protect providers from arbitrary and capricious actions that may occur during the auditing process and hold the government accountable for guidance it gives to providers.

"The focus of these provisions is to try to provide greater beneficiary and provider education and to make revisions to the provider appeal and overpayment recoupment process," notes Robert Rabecs, an attorney with Hogan & Hartson LLP (Washington, D.C.). "For the most part, they are not controversial and will help reduce some of the administrative burden on providers."

One change that could

➥ *p. 11*



Larry Small

Medicare Coding Changes, *from p. 1*

282.42, 282.42 and 282.49. Code V43.2 is replaced with V43.21 and V43.22. Several new codes are added – 282.64, 282. 68 and 289.52.

- In the urine culture bacterial NCD list of covered diagnoses, code 600.0 is replaced with 600.00 and 600.01; code 600.1 is replaced with 600.10 and 600.11; code 600.2 is replaced with 600.20 and 600.21; code 600.9 is replaced with 600.90 and 600.91. The following new codes are added: 780.93, 780.94, 785.52 and 788.63.

Ensure Coding Accuracy

The new requirement that lab claims contain a valid ICD-9 code will require hospital and independent labs to step up efforts to obtain accurate diagnostic information from physicians, says Larry Small, director of compliance and billing services for PCS Laboratory Services Group (Ann Arbor, MI).

"What we're seeing here is a heightened effort by the government to ensure that all claims have medical necessity justification," notes Small. While many labs already have required that physicians provide ICD-9 codes on lab requisitions, some have continued to accept narrative diagnoses and have then assigned codes.

In some cases, labs have used v72.6, a general code for laboratory testing, when physicians failed to provide adequate diagnostic information. That code probably will no longer be acceptable, warns Small.

According to CMS, claims must include codes that provide the highest degree of accuracy and completeness and reflect the highest degree of specificity. "In the context of ICD-9-CM coding, the 'highest degree of specificity' refers to assigning the most precise ICD-9-CM code that most fully explains the narrative description of the symptom or diagnosis," states transmittal B-03-045.

"I wouldn't advise using v72.6 since it doesn't refer to a symptom or diagnosis," advises Small. "Labs should be contacting the doctor whenever they receive a Medicare test request where a symptom or diagnosis has not been given."

Labs must work with physicians to improve compliance, but in cases where a physician refuses to provide adequate diagnostic information, a lab may have to take stronger action, he says. "If a doctor says 'I'm not going to do this,' you may have to begin charging the doctor for your services," explains Small. When faced with this option, most physicians will begin providing the required diagnostic information, he notes.

Resources

- Larry Small: 727-866-1311
- CMS Program Memos B-03-045, B-03-046, AB-03-091 and AB-03-104, available at *www.cms.hhs.gov/manuals/memos*.

Tenet Healthcare Troubles Continue, Company Beefs Up Compliance Program

The troubles at Tenet Healthcare, the nation's second largest for-profit hospital chain, seem to just keep getting worse. The Santa Barbara, CA-based-company, which has been the target of several federal investigations over the past year, revealed in August that Florida Medicaid officials have launched a new probe into its hospital ties.

The disclosure of the Florida investigation came just days after the company agreed to pay $54 million to settle criminal and civil charges involving one of its hospitals, Redding Medical Center. Two cardiac surgeons at Redding, Drs. Chae Hyun Moon and Fidel Realyvasquez, were accused of performing thousands of unnecessary invasive coronary procedures, including heart catheterizations, angioplasty and open heart surgeries.

> ***"There's nothing particularly unique about Tenet in terms of its practices. The company is attracting so much government attention primarily because of its size." – Bradley Tully, Esq.***

The settlement represents "the largest recovery in the history of the United States Department of Justice in a case alleging lack of medical necessity," according to the U.S. attorney for the Eastern District of California.

Bradley Tully, Esq.

In an Aug. 6 statement on the settlement, Tenet noted that it did not include "any admission of wrongdoing by Tenet, its subsidiaries or Redding Medical Center." Tenet also said the company and its subsidiaries "expressly deny that they knowingly submitted false claims to Medicare and other government healthcare programs for unnecessary cardiac procedures at Redding."

More Problems

Tenet officials revealed the Florida investigation in an Aug. 7 filing with the Securities & Exchange Commission. According to the company, the Florida Medicaid Fraud Control Unit issued an investigative subpoena June 6 "seeking employee personnel records and contracts with physicians, therapists and management companies, including loan agreements and purchase and sale agreements." Tenet says it's cooperating with the investigation, which covers records for the past 11 years.

The most recent Tenet woes come on the heels of a July 17 indictment of Tenet, Alvarado Hospital Medical Center (San Diego, CA), a subsidiary, and Alvarado's CEO Barry Weinbaum on criminal charges relating to physician relocation payments. The 17-count indictment claims that Weinbaum provided kickbacks to physician groups who took in new doctors and referred patient business to Alvarado.

Tenet has maintained its innocence, saying the physician location agreements were "entirely appropriate under the law" and that specific agreements were designed to help Alvarado "meet a demonstrated need" for additional or specialized healthcare resources in the community.

"We believe this very broad indictment mistakenly attacks a well-established, lawful and common means by which U.S. hospitals attract needed physicians to their communities," said Tenet President and Acting CEO Trevor Fetter.

Bradley Tully, a partner with the law firm of Hooper, Lundy & Bookman (Los Angeles) believes the government's charges on Tenet's physician recruiting practices could signal a willingness to look at recruiting practices at other hospitals.

"It's bit of a puzzle as to why [Tenet] got in trouble, but it is attracting attention," he says. "The legitimacy of physician recruiting has always been somewhat up in the air. Case law is somewhat unclear. However, we are advising providers to review their recruiting arrangements and make sure they're comfortable with them."

Company Beefs Up Counsel

Tenet said Aug. 4 that it has undertaken efforts to improve compliance by appointing a new compliance officer and hiring a team of legal advisors. Tenet's former senior counsel, Cheryl Wagonhurst, has been named chief compliance officer, and D. McCarty Thornton, former chief counsel for the Department of Health and Human Services Office of Inspector General, has been hired as a special advisor to Tenet's compliance department. Thornton currently heads the healthcare regulatory practice group at Sonnenschein Nath & Rosenthal LLP in Washington, D.C.

Other advisors who will be working with Thornton include Howard Young, also with Sonnenenschein and a former division chief in the OIG's civil recoveries unit, and T. Reed Stephens, who worked for eight years in the civil fraud section of the Justice Department's civil division.

Resources

Tenet Healthcare: 805-563-7000
Bradley Tully: 310-551-8111

Court Increases Prison Term For Former Damon Exec

Thurston Sentenced To 5 Years Jail Time

A federal appeals court Aug. 4 increased to five years the prison sentence of William Thurston, a former executive of Damon Clinical Laboratories Inc., who was convicted of defrauding the Medicare program of more than $5 million.

The U.S. Court of Appeals for the First Circuit agreed with federal prosecutors that a district court judge had been too lenient in June 2002 when he sentenced Thurston to three months in prison followed by three years of supervised release. The lower court judge, Edward Harrington, reasoned that the sentence should have been lower than called for under federal guidelines because of Thurston's charitable works and because Damon President Joseph Isola had received a sentence of three months' probation for his part in the overbilling scheme.

Thurston, a former vice president of Damon, was convicted in December 2001 of filing false and fraudulent claims for medical tests. He was charged with participating in a scheme in which physicians were tricked into ordering unnecessary blood tests, paid for by Medicare. Company officials devised the plan in response to a cost-cutting, across-the-board fee reduction for laboratory tests instituted by Medicare in 1988, prosecutors alleged.

Thurston was one of four Damon executives alleged to have participated in the scheme. Isola pleased guilty to one conspiracy count in July 2000 and cooperated with the government, one defendant died before trial and the trial judge dismissed charges against another defendant. Charges that Thurston had unlawfully bundled apolipoprotein and kidney dialysis tests were dismissed.

The lower court erred in its sentencing, ruled Judge Sandra Lynch in overturning the lower court ruling. "Thurston was convicted of a serious crime, a massive fraud at public expense involving deceit, trickery and sophistication," she wrote. "A five-year imprisonment in light of the nature of the crime reflects the seriousness of the offense, the need for congruity with 'blue collar' crime and the need to deter other executives from similar law-breaking."

COMPLIANCE PERSPECTIVES

Responding to a HIPAA Investigation: A Primer for Covered Entities

Marc Goldstone, Esq., is an attorney in the health law division of Hogland, Longo, Moran, Dunst & Doukas, LLP, New Brunswick, NJ.

On Apr. 14, 2003, HIPAA's final privacy rule became effective. As a practical matter, healthcare providers, health plans and healthcare information clearinghouses that transmit certain electronic transactions (collectively, covered entities, or CEs) have had more than two years notice to implement their HIPAA compliance plans, so as to ensure adherence to the privacy rule's requirements. However, as the "rubber meets the road," there are sure to be undiscovered gaps in privacy practices. Those gaps could be the basis for a government investigation into a covered entity's HIPAA procedures.

Development of an investigation response policy is one key to minimizing a CE's liability for HIPAA violations. The Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services has noted that to the extent practical, it will seek the cooperation of covered entities in obtaining compliance with the privacy rule and may provide technical assistance to help covered entities voluntarily comply. Enforcement activities will focus on obtaining voluntary compliance through technical assistance, and OCR will seek to resolve matters by informal means before issuing findings of non-compliance (68 FR 18897).

Based on this, it appears as if the focus of the civil HIPAA enforcers will be to ensure compliance through assistance to covered entities; not through threats of legal action (at least, during the initial phases of an investigation). Given this stance, it would seem foolish for a CE not to work with OCR to some extent if OCR representatives come to an entity's place of business with an official inquiry. Why skip negotiation and go straight to punishment?

So, what should a covered entity do if government officials "drop by" their offices one day for an official HIPAA chat?

Step 1: ***Don't panic.*** Really. It's important to keep calm when the investigators are at your door. The reason for this is simple—prosecutors "like" nervous interviewees. They like them so much that they often invite them back to the home office for a more in-depth discussion. Each covered entity should choose a liaison for investigations; that liaison should be someone who has a cool demeanor under pressure. If a covered entity's key executive does not possess this trait, top execs should select another manager or employee to serve in this key position. The investigation liaison serves as the covered entity's "face" during the investigation; make sure it is a good one.

Step 2: ***Expect the unexpected.*** Remember, anyone may file a complaint with OCR, and the complainant need not notify the CE before filing. Technically, complaints must be filed within 180 days of when complainant knew or should have known of the violation. Be aware, however, that HHS can extend this time period for "good cause shown." While OCR reps "will generally" give notice before requesting access to a CE's books and records, they are not required to do so (65 FR 82602). Thus, a CE's compliance staff should be ready to respond to an investigation out of the blue. It might even be prudent to hold an "investigation drill" periodically to ensure readiness.

Step 3: ***Phone home.*** Each covered entity should have a "phone tree" that should be activated whenever an investigation occurs. The designated communicator should call:

- Your Attorneys (HIPAA counsel *and* local counsel, if they aren't the same)
- Your Executive Management
- Your Privacy Officer
- Your Security Officer
- Your Compliance Officer
- Your Health Information Management Department/Custodian of Records

Everyone on this list needs to know that "the wolf is at the door" and should get the word from someone official, rather than through the grapevine. It's best if you immediately assign someone to make these calls (as part of a well-crafted "responding to investigations" policy that should apply to *all* official inquiries, not just HIPAA) *out* of sight and hearing of the investigators; you'll likely be too busy doing other things, and you really don't want to make the calls in front of them.

Step 4: ***Know what's in store.*** Forewarned is forearmed. We know that OCR's enforcement activities will include:

- working with covered entities to secure *voluntary compliance* through the provision of technical assistance and other means;
- responding to questions regarding the regulation and providing interpretations and guidance;
- responding to state requests for exception determinations;
- investigating complaints and conducting compliance reviews;
- seeking civil monetary penalties and making referrals for criminal prosecution (where voluntary compliance cannot be achieved).

It's also important to know how enforcement initiatives will originate. OCR has stated that "[t]he [investigation] process will be complaint-driven and consist of progressive steps that will provide opportunities to demonstrate compliance or submit a corrective action plan" (68 FR 18897). "Complaint-driven" means that unhappy patients, disgruntled employees, former employees, competitors and others with an ax to grind will likely initiate HIPAA investigations.

Step 5: ***Take appropriate action.***

- Cooperate (but cautiously). Ask for the official government agency-issued identification of the investigators (business cards are *not* official identification). Write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. If they can't produce acceptable I.D., call your attorney immediately and defer the provision of any PHI until after you confer with counsel or until the investigators produce acceptable I.D. *Be sure* that you've made appropriate requests for I.D. and that they've been unreasonably refused before you do. If you choose this route, be sure to have one or two witnesses who can vouch for your request.
- Ask for the name and telephone number of the lead investigator's supervisor, but only if, in your judgment, his/her demeanor indicates that you can ask such a question without engendering "hard feelings." Under *no* circumstances should you take any action to escalate tensions, except if you genuinely doubt the identity or authority of the investigators. If you can obtain this information, your attorney will thank you for it, because it will prove an invaluable "short-cut" to obtaining information about the investigation and may potentially clear the way to a settlement in short order, if advisable (thus, reducing your legal fees).
- Be sure to determine if there are any law enforcement personnel present *(i.e.*, FBI, US Attorney investigators, state prosecutor investigators, etc.). Again, this is information that will be invaluable to your attorney (if law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation).
- *Do* permit the investigators to have access to protected health information (PHI), in accordance with your notice of privacy practices (NPP), and federal and state law. Once investigators have verified their identities and verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them if the PHI sought is the subject matter of the investigation, or reasonably related to the investigation. Ask them to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes and document their responses in your own written records. Again, have at least one witness with you when you ask about their authority to access PHI. All witnesses should prepare a written summary of the conduct and communications they observed as soon as possible; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed and the witnesses signature.
- Send your staff employees elsewhere, if possible. There is absolutely no requirement that you provide witnesses to be ques-

tioned by the government during the initial phases of the investigation; likewise, there is no need for you to connect the investigators with any disgruntled employees. If necessary, give your employees the rest of the day off; but do whatever you have to do to send them away and keep them away. Unless the investigators subpoena your employees (which they probably won't do until after the initial visit) you likely have no federal duty to line up your employees for questioning at this point (although state laws may vary on this; check with your local counsel for more specific info.). *Do not* instruct your employees to hide or conceal facts, or otherwise mislead investigators—that's obstruction of justice and is a crime in and of itself.

- Ask the investigators for documents related to the investigation, such as:
  - copies of any search warrants and/or entry and inspection orders
  - copies of any complaints
  - a list of patients they are interested in
  - a list of documents/items seized
- Don't leave the investigators alone, if possible. Assign someone to "assist" each investigator present.
- Don't be *too* solicitous. Don't offer food (coffee, if already prepared, and water, if already available, is probably ok) or anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment. For example, don't offer to buy investigators lunch. Don't get "chatty." Although OCR has indicated it is here to help, these investigators aren't your friends; only tell them what you are required by law to reveal. Defer to the advice of counsel if you are unsure. Don't be uncooperative or exhibit a poor attitude; do answer direct questions fully and to the best of your ability. Don't offer opinions, don't talk about your competitors and don't complain about the burdens associated with HIPAA compliance *or* the government.
- Notify your State Practice Association, if you feel comfortable, to help spread the word about local enforcement activity, as well as to obtain assistance. Most state associations have a government relations coordinator who has contacts that may be valuable to a covered entity under investigation; the only way to access those contacts is to make the call.

Step 6: ***Know what they can do to you.*** It's important to know the potential consequences of a HIPAA investigation, before deciding what your response will be. If OCR reps determine that a CE has committed a HIPAA civil violation, they will:

- Inform the CE (in writing).
- Inform the complainant (if any, in writing).
- Attempt to resolve the matter by informal means whenever possible (per the enforcement rule).
- Issue a written noncompliance finding if the issue cannot be informally resolved. (Remember that OCR enforces civil violations of the privacy rule; criminal issues are referred to OIG and the Department of Justice).
- If no violation is found, OCR will inform the CE and the complainant, if any (nothing says this notification must be in writing).

Step 7: ***Know HHS' limitations.*** Every CE should be aware that:

- Civil monetary penalties cannot be imposed in respect of acts that constitute a "HIPAA Crime" (42 USC 1320d- 5(b)(1)).
- A CMP may not be imposed if "it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision" (42 USC 1320d- 5(b)(2)).
- A CMP may not be imposed if the failure was due to "reasonable cause and not to willful neglect" (42 USC 1320d- 5(b)(3)).
- A CMP may be *reduced* or *waived* "to the extent that the payment of such penalty would be excessive relative to the compliance failure involved" (42 USC 1320d- 5(b)(4)).
- HHS may *not* initiate a CMP action "later than six years after the date" of the occurrence that forms the basis for the CMP (68 FR 18896).
- CMP actions are *not* summary; the person upon whom HHS seeks to impose CMPs *must* be given the written notice and an opportunity for a hearing on the record,

HIPAA Penalties

- If the violation is egregious enough to constitute a crime, DHHS will impose criminal fines up to $50,000 and/or 1 year in jail.
- If the crime involves obtaining, using and/or disclosing PHI under false pretenses, the penalty can include a fine of up to $100,000 and/or 5 years in jail.
- If the crime involves the intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm, the penalty can include a fine of up to $250,000, and/or 10 years in jail.

during which the person may be represented by counsel, may present witnesses and may cross-examine witnesses (42 U.S.C. 1320a-7a(c)(2)).
- ❖ HHS *cannot* impose a HIPAA CMP on anyone who is *not* a covered entity (68 FR 18898).

Step 8: ***Know when to hold 'em, and know when to fold 'em.*** Sometimes, it just makes sense to settle charges of a HIPAA violation. There is a specific process to settle a case, though, and it is important to follow the procedures to the letter:

- ❖ HHS can "settle any case or … compromise any penalty during the process" (68 FR 18898, referencing 45 CFR Part 160.510).
- ❖ Factors to be taken into account by OCR when making a settlement determination will be "addressed in the notice-and-comment rulemaking" planned for the remainder of the enforcement rule (68 CFR 18899).
- ❖ If HHS notifies a CE of a proposed penalty, the respondent *must* request a hearing *in writing and in a timely manner* or the penalty becomes final and the respondent has "no right to appeal." In general, the CE has 60 days after notice of the proposed penalty determination is received by the respondent (68 FR 18899, referencing 45 CFR Part 160.516). Receipt date is "presumed" to be 5 days after the date of the notice. Hearings will be on the record, discovery is limited, and depositions/interrogatories are specifically prohibited.
- ❖ Decision of the ALJ is the decision of HHS (45 CFR Part 160.564 (d)). This is contrary to many state administrative law systems, where an ALJ's decision can be adopted, modified or rejected by the head of the administrative agency. However, judicial review of final penalty decisions is authorized, and the respondent may request a stay pending judicial review.

It's important to remember that OCR is a relatively "new animal" to those of us in the healthcare field. We have some experience with OIG investigations, but we're just not sure how OCR will treat us. A strong, effective compliance plan and a well-crafted response to investigations policy will be your best tools to survive a HIPAA investigation and not get trampled by the HIPAA HIPPOs (Health Information Protection Police Officers).

Marc Goldstone, Esq., can be reached at Hoagland, Longo, Moran, Dunst & Doukas, LLP, 40 Paterson St., P.O. Box 480, New Brunswick NJ 08903. Tel: 732-545-4717. E-mail: mgoldstone@hoaglandlongo.com.

What To Do Before An Investigation

- ❖ Implement your HIPAA Compliance Plan to the greatest extent; if you take reasonable and scalable steps to comply, you can make all of your "incidental disclosures" permissible pursuant to the final privacy rule, and thus, they will not constitute HIPAA violations.
- ❖ Document the steps that you took to implement your plan; HIPAA committee minutes (if you have a HIPAA compliance committee) should be maintained in writing.
- ❖ Document the monies you spent in implementing the plan; save budgets and receipts.
- ❖ If you made any cost/benefit "reasonableness" determinations regarding specific plan elements, document them and have that documentation available for inspection.
- ❖ Periodically examine reports to your Privacy Office/HIPAA Hotline.
  - — Investigate *all* reports and conclude *all* investigations with *written* documentation.
  - — Trend all your reports; if there are discernible trends, conclude them with written documentation.
  - — Revisit the trends over time to see if your solution is effective; if not, revise the solution and try again.
- ❖ Keep your disclosure logs in good order (especially with respect to inappropriate disclosures—this is where complaints are *very likely* to originate; you don't want it to appear that you "covered-up" anything).
- ❖ Train, educate, explain and then train some more.
- ❖ Maintain employee training time records, training funds expended and training materials used. Make sure each employee takes and passes a HIPAA training post-test. If they fail, retrain them and test again.
- ❖ Read the latest OCR HIPAA implementation and enforcement guidance at: *http://www.cms.hhs.gov/hipaa/hipaa2/education/infoserie/*
- ❖ Watch the online enforcement video from OCR, at *http://www.ehcca.com/streaming/index.html*. This is great guidance from Robinsue Froboese, J.D., Ph.D., Deputy Director, Office of Civil Rights
- ❖ Include HIPAA in your policy for responding to official investigations (Don't have a policy for responding to investigations? Now's the time to get one).
- ❖ *Don't* include the OCR address in your NPP (you don't have to; you just have to tell patients how to get it. If they have to contact you to get it, then you may have the opportunity to resolve the complaint; at the very least, you'll be on notice of a potential complaint).
- ❖ Get and rely on the written advice of counsel and consultants (at best, they'll be right; at worst, you can be indemnified by their professional liability policies). Due diligence is important in developing an effective HIPAA compliance plan.

Take Final Steps To Prepare for HIPAA TCS Implementation

New Standards Effective Oct. 16, 2003

With less than two months to go before new national standards for electronic health care transactions become effective, healthcare providers should be taking final steps now to ensure compliance, advises the Centers for Medicare & Medicaid Services.

The new standards, mandated by the Health Insurance Portability & Accountability Act of 1996 (HIPAA) take effect Oct. 16, 2003. After that date, all covered entities (CEs), including health plans, may not conduct non-compliant transactions.

For more information on HIPAA compliance, go to www.cms.hhs.gov/hipaa/hipaa2

CEs should already have been working toward becoming HIPAA compliant by reviewing business operations, assigning a HIPAA point person, identifying HIPAA partners, testing health plans and payers and researching options, says CMS in recent guidance posted on its website.

If you are a small provider who does not conduct any of the HIPAA electronic transactions (and you do not have a billing service or clearinghouse conduct HIPAA electronic transactions on your behalf), you may not be affected by HIPAA. To find out if you are covered, review the CMS information paper, "Are you a covered entity?" and the "Covered Entity Decision Tool," both of which are available on the CMS website

If a CE's software vendor or current billing service is unable to ensure HIPAA-compliant transactions after Oct. 16, CMS advises the CE to consider using an alternative vendor or clearinghouse that is HIPAA compliant. (If you bill Medicare directly, you can obtain special software free or for a small charge. More information is available at *www.cms.hss.gov/providers/edi*).

CMS emphasizes that it intends to focus on voluntary compliance and use a complaint-driven approach for enforcement of the TCS standards. When the agency receives a complaint about a covered entity, it will notify the CE in writing that a complaint has been filed. The CE will then have the opportunity to demonstrate compliance, document its good-faith efforts to comply with the standards and/or submit a corrective action plan.

Questions to Ask Vendors, TPAs Or Clearinghouses

Entities covered by HIPAA should communicate often with their software vendors about their progress toward compliance, says the Centers for Medicare & Medicaid Services in recent guidance to providers.

"For instance, your vendor should supply you with upgraded software that will allow you to conduct electronic transactions according to HIPAA standards come Oct. 16, 2003," recommends CMS in guidance posted on its website. "They should also be testing their software with you and your payers."

Entities that use a clearinghouse, billing service or third-party administrator (TPA) should stay abreast of their HIPAA activities. Don't assume they are HIPAA compliant, warns CMS, which advises asking the following questions:

1. Are you working on developing software to meet your HIPAA needs?

Specifically,

—What HIPAA transactions does your product support? Claims and encounter information? Payment and remittance? Claims status inquiry? Referral and authorization inquiry?

—Which products do you now sell or support currently, which *will not* be supported after Oct. 16 or will not be HIPAA compliant?

—What software updates are needed for HIPAA compliance?

—Does my office need a particular release of your software to implement the HIPAA transactions or is an entire upgrade from the current version required?

—Can I upgrade to the various electronic

transactions incrementally?
—What is the minimum hardware requirements for servers and workstations to run the HIPAA compliant version?
—When will the software update be available?
—What training, support and services are available to help my office?
—Do you charge extra for training and support services?
—How do you remain current on the latest HIPAA developments? Do you belong to any of the HIPAA-related workgroups?
—Who specifically can I contact for HIPAA electronic transactions questions?

2. Will your software be able to support HIPAA transactions and code set requirements?

Specifically,
—Do you use the official Implementation Guides for HIPAA transactions? Is your software using the latest version of the guides (4010A)?
—Do you have the companion guides for my payers with whom I file directly?
—How does your product support collecting the required and situation claim data?
—Will your software support the required HIPAA code sets for medical and non-medical?
—Is there a process for cross-walking from current codes to the HIPAA mandate codes?
—What new data will I need to start collecting?
—Are there any edits built into your software?
—Do you have a price list for the various upgrades, or new version of software?
—How can we submit transactions directly to you? Are there any changes in connectivity? (for clearinghouses)

3. What are your electronic transactions and code set testing plans?

—How much lead time is required to install and test the software?
—How will current claims processing with existing formats proceed while testing new ones?
—Has your testing process included all of the seven types recommended by WEDI SNIP?
—Has the software received third-party certification that it can generate HIPAA compliant transactions?
—Will you send me a testing schedule that includes internal testing, testing with Medicare, testing with commercial payers and testing with a clearinghouse (if applicable)?
—Have you tested successfully with any of my payers? Which ones?
—What are your contingency plans if you cannot be ready on time?

Rural health centers, hospices and other medical facilities will be required to electronically submit annual Medicare cost reports beginning in May 2005, according to the Centers for Medicare & Medicaid Services (CMS). Hospitals, skilled nursing facilities and home health agencies already have to file cost reports electronically.

According to a notice published the Aug. 22 *Federal Register*, the new requirement will affect rural health centers, hospices, organ procurement organizations, federally qualified health centers, community mental health centers and end-state renal disease facilities. The new requirement will be phase in over a two-year period, during which electronic claims will not be rejected. However, fiscal intermediaries will contact providers about problems during the phase-in period so that corrections can be made.

CMS will provide free software to providers who are financially unable to purchase software necessary to comply with the rule, the agency says. The software should be available by Sept. 30, 2004. Providers who use the free software, however, will be "required to manually complete the cost report and to manually determine the final settlement," notes CMS.

Robert Rabecs

Medicare Reform, *from p. 1*

create some problems, at least initially, is a provision that requires the transfer of Medicare administrative law judges (ALJs) from the Social Security Administration to the Department of Health and Human Services, says Rabecs. "They're moving from one bureaucratic framework to another. I'm sure there will be some problems with the start-up since we're talking about potentially new ALJs handling these issues," he explains.

Regulatory Changes

The compromise contains a number of regulatory and contracting reform provisions. In part, the conference agreement:

- ❖ Requires establishment by regulation of payments for new lab tests.
- ❖ Requires Medicare secondary payer data collection criteria to be the same for hospitals and independent labs performing reference lab tests.
- ❖ Prohibits the introduction of new material in final rules without an opportunity for public comment.
- ❖ Prohibits retroactive application of new regulations and policies.
- ❖ Requires a waiting period of 30 days after the announcement of a substantive change before it can become effective.
- ❖ Prohibits sanctions if a provider follows written, erroneous guidance from the government and its agents.
- ❖ Creates a competitive process for contracting for Medicare administrative functions such as processing and paying of claims.
- ❖ Establishes standards for random prepayment reviews, establishes limits on the use of non-random prepayment review and requires notification at the end of a prepayment review.
- ❖ Allows providers up to three years to repay overpayment in cases of hardship (five years if extreme hardship).
- ❖ Prohibits recovery of overpayments during an appeal until after an evaluation by an independent party.
- ❖ Prevents extrapolating overpayments, based on a small sample of claims, to a larger number of claims unless a sustained or high level of payment error has been identified, or unless documented education intervention has failed to correct the problem.
- ❖ Requires Medicare contractors, within the context of a consent settlement, to notify a healthcare provider of the nature of problems identified and what steps the provider should take to address the problems before an overpayment projection may be made from a probe of sample claims.
- ❖ Ensures that underlying billing mistakes can be corrected by permitting providers to submit supporting documentation.
- ❖ Requires that contractors notify providers when they overuse a particular code.
- ❖ Requires that providers are notified in writing of post-payment audits and that a full review and explanation of all audits be made available to providers, except where fraud is suspected.
- ❖ Requires the Secretary to establish a process for provider enrollment and establishes hearing rights for disenrolled providers.
- ❖ Requires the Secretary to develop a process to allow providers to correct minor errors or omissions in submitted claims without having to initiate an appeal.

Controversial Provisions

Negotiators have yet to address some of the more controversial provisions that will affect healthcare providers, says Rabecs. For example, the Senate Medicare reform bill contains some changes to fraud and abuse mandates that are not included in the House version of Medicare reform, such as an increase in civil monetary penalties (*GCR, Aug. 03, p. 9*).

"One of the more significant areas addressed in the Senate bill but not the House bill is the provision on specialty hospitals," he adds. The provision would narrow the exception currently contained in the Stark ban on physician self-referrals that allows physicians to have an ownership interest in specialty hospitals if the physicians practice in the hospitals. The Senate bill would prohibit physician referrals to most specialty hospitals in which they have financial ownership.

The House bill, meanwhile, calls for the Medicare Payment Advisory Commission to conduct a comparison study of specialty and general acute care hospitals to determine if there are excess self-referrals to niche hospitals, the differences in quality of care the impact of specialty facilities on general hospitals and the differences in services provided.

Resources

Robert Rabecs: 202-637-5842
House Ways & Means: 202-225-8933

Lab Complaints: The Centers for Medicare & Medicaid Services (CMS) is considering establishing a new records system to track and process complaints and incidents involving laboratory providers and suppliers. According to an Aug. 22 *Federal Register* notice, the ASPEN Complaints/Incidents Tracking System (ACTS) is a windows-based program designed to track and process complaints and incidents reported against health care facilities regulated by CMS under the Clinical Laboratory Improvement Amendments of 1988. ACTS would track allegations of complaints made against providers and suppliers and maintain information on laboratory directors and owners. Specific fields are configurable by individual states to accommodate a variety of operations environments, CMS says.

FCA Backlog: Sen. Finance Committee Chairman Charles Grassley (R-Iowa) has asked government lawyers to explain the recent doubling in the backlog of unresolved whistleblower cases. In an Aug. 4 letter to William Reukauf, acting special counsel with the Office of Special Counsel (OSC), Grassley said the backlog at OSC more than doubled in the past 18 months. Grassley requested a full briefing from OSC, giving the reasons for the doubling, along with a plan of action that would reduce the backlog in the short term and identify and address systematic weakness to prevent future backlogs.

Abbott CIA Online: The corporate integrity agreement negotiated between Abbott Laboratories and the Department of Health and Human Services Office of Inspector General (OIG) is now available online at *www.oig.hhs.gov*, under "What's New." Abbott was required to enter into a five-year CIA as part of a recent settlement stemming from a probe into the marketing of adult nutritional products administered through feeding tubes in hospitals and nursing homes (*GCR, Aug. 03, p. 3*).

G-2 Compliance Report (ISSN 1524-0304). © 2003 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.