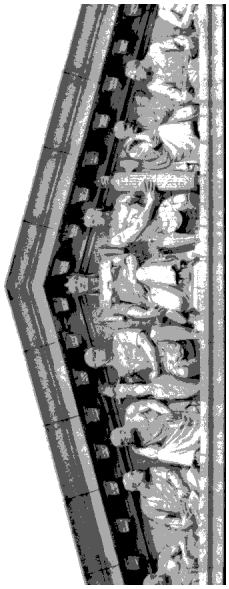

G-2 Compliance Report

WASHINGTON G-2 REPORTS

Vol. II, No. 7, August 2001

For Hospitals, Laboratories and Physician Practices

Privacy Guidance Eases Some Provider Fears
More Changes To HIPAA Standards Promised

Initial federal guidance on the patient privacy rules promulgated under the Health Insurance Portability & Accountability Act (HIPAA) should allay some fears of healthcare providers and health plans about how far they have to go, say experts.

The guidance, released July 6 by the U.S. Department of Health & Human Services (HHS), explains and clarifies key requirements published last December and scheduled to take effect Apr. 14, 2003 (small health plans have an additional year).

Christina Kennedy, an attorney with Foley & Lardner (Orlando, FL), believes HHS's lengthy document goes a long way toward answering many of the questions providers and plans have about their responsibilities.

"The guidance not only provides clarification of the regulations, which some of us found to be somewhat ambiguous, but it also softens them because it uses a reasonable standard for many of the provisions," she says. "It really clarifies that many of the things that physicians and other providers do on a daily basis, such as using sign-in sheets and calling out patients' names in waiting rooms, will still be allowed."

Bob Mirimonte, senior consultant in HIPAA/e-Health for SSM Healthcare (St. Louis, MO), agrees that the guidance is useful, but maintains that much of what it spells out is common sense. "There really weren't any surprises, but it did reinforce many of our interpretations of the regulations."

Continued on p. 2

Physicians Snared In Kickback Crackdown

In what it calls the most significant use to date of its authority to impose civil money penalties (CMPs) for kickbacks, the HHS Office of Inspector General has imposed CMPs on six physicians who either paid or received illegal kickbacks for referrals of Medicare patients.

In settling with the government, the doctors collectively paid more than $390,000, and one agreed to be excluded from federal healthcare programs for four years.

Five of the settlements resolved civil charges against Florida physicians who referred patients to Clearwater Clinical Laboratory and other diagnostic service companies in the Tampa Bay area.

"This is the most notable civil money penalty enforcement action under the anti-kickback statute to date," says Gabriel Imperato, an attorney with Broad & Cassel in Ft. Lauderdale. Imperato represented one of the physicians.

"In theory, criminal prosecution is still possible, although as a practical matter, it's unlikely," he adds. "In these cases, the civil alternative

Continued on p. 10

Inside this issue

Privacy Guidance, *from page 1*

Perhaps most useful, he believes, is the clarification that a provider needs to obtain patient consent for use or disclosure of protected health information (PHI) only one time, "regardless of whether there is a connected course of treatment or treatment for unrelated conditions."

"We were never really sure how often we had to obtain consent," says Mirimonte. "This does create more of a tracking problem though, especially if a patient has been treated under a different name. We may require consent each time a patient comes to the hospital."

Guidance Highlights

Another important clarification concerns conversations between physicians or other healthcare personnel and patients. The guidance specifies that hospitals don't have to retrofit rooms to make them private and soundproof to prevent conversations about the patient's condition from being overheard. According to HHS, the rule simply requires that reasonable safeguards be used, such as curtains, screens, or similar barriers often already in use.

The guidance further clarifies that a friend or relative may pick up a patient's prescription at the pharmacy. And in emergency situations, providers may give treatment without first obtaining consent if the provider believes that a delay would compromise the patient's care.

The HHS guidance is the first of a series of promised technical assistance documents to help providers and consumers. HHS also plans to use the formal rulemaking process, subject to public comment, to propose additional modifications to the privacy rules prior to the compliance date in order to correct any unintended negative effects on healthcare quality or access to care. Among expected changes:

- ***Allowable communications:*** HHS will make clear that covered entities are free to engage in whatever communications are required for quick, effective care, including routine oral communications with family members, treatment discussions with staff involved in coordinating patient care, and using patient names to locate them in waiting areas.
- ***Phoned-in prescriptions:*** Pharmacists will be allowed to fill prescriptions phoned in by a patient's doctor before obtaining the patient's signed consent.
- ***Referral appointments:*** Direct treatment providers receiving a first-time patient referral will be allowed to schedule appointments, surgery, or other procedures before obtaining the patient's signed consent.
- ***"Minimum necessary" standard:*** HHS will clarify that certain common practices, such as use of sign-up sheets and x-ray lightboards, and keeping a patient's medical charts at the bedside, will not be prohibited.

More Clarification Needed

While the guidance does clear up some confusion, Kennedy believes additional clarification is needed in a few areas, including conditions under which PHI may be used or disclosed by covered entities for research purposes and the responsibilities of hybrid organizations.

Under the privacy rules, researchers must obtain individual authorization to disclose PHI for research or, absent individual authorization, must obtain approval from an Institutional Review Board (IRB) or a Privacy Board. A covered entity may always use or disclose, for research purposes, health information that has been stripped of individual identifiers.

"It's not clear in the regulations whether the information that can be used for research is as broad as most researchers would like," says Kennedy. "Not everyone has IRBs and not everyone will be able to create a Privacy Board that's acceptable under the standards. I would like to see standards for research when those things don't exist."

HHS should also provide greater detail on how the privacy rules will affect large employers and corporations with self-funded group health plans, Kennedy believes. "A lot of corporations aren't aware that HIPAA is going to affect them because they're not, *per se*, in the health industry."

Resources

- Christina Kennedy: 407-423-7656
- Bob Mirimonte: 314-994-7932

Privacy FAQs

To help clear up common misconceptions about the HIPAA privacy requirements, the initial HHS guidance includes a number of frequently asked questions. Here's a sample of just a few. The complete guidance is posted online at www.hhs.gov/ocr/hipaa.

Q *Will the consent requirement restrict the ability of providers to consult with other providers about a patient's condition?*

A *No. A provider having a direct treatment relationship with a patient would have to have initially obtained consent to use that patient's health information for treatment purposes. Consulting with another healthcare provider about the patient's case falls within the definition of "treatment" and, therefore, is permissible. If the provider being consulted does not otherwise have a direct treatment relationship with the patient, the provider does not need to obtain the patient's consent to engage in the consultation.*

Q *May consent for use or disclosure of protected health information be provided electronically?*

A *Yes. The covered entity may choose to obtain and store consents in paper or electronic form, provided that the consent meets all requirements under the privacy rules, including that it be signed by the individual. Paper is not required.*

HIPAA Privacy Standards: Tips On Addressing Special Concerns

This is the second of two articles on integrating patient privacy protections under the Health Insurance Portability & Accountability Act (HIPAA) into your existing compliance program.

Once you've begun taking steps to integrate HIPAA privacy requirements into your existing compliance program, the next move is to tackle special concerns, such as how the standards affect contractors and how they apply to patients participating in research, says Carrie King, chief compliance officer for the University of Texas M.D. Anderson Cancer Center in Houston.

Business Associates

This term generally encompasses individuals or businesses—such as attorneys, consultants, or financial advisors—who are doing something for your organization that you would normally do yourself, King explains.

"If your doctors are in-house, and they're a part of you, they are not business associates. However, if you don't 'own' your doctors, if you have doctors in the community, does that alone make them business associates? No. Could it make them business associates? Yes, if the hospital provides the billing services for the physicians. So you need to define the relationships you have."

Once you've determined who qualifies as business associates, you should begin incorporating HIPAA language into your contracts with them, King advises. M.D. Anderson, for example, has already begun putting contractors on notice that they may be required to provide assurances that they will handle protected health information in compliance with HIPAA privacy standards.

"Not everyone will qualify as a business associate, but you do have to get people to start thinking in those terms so they don't panic when the time comes."

Medical Research

Organizations involved in medical research have to meet slightly different privacy standards under HIPAA, notes King. In general, the "Common Rule," which dictates the criteria for Institutional Review Board (IRB) approval of research, will apply.

To obtain a waiver from compliance with HIPAA requirements, the organization must demonstrate that:

- Use or disclosure of protected health information involves no more than minimal risk;
- The waiver will not adversely affect privacy rights and welfare;
- The research could not practically be conducted without the waiver;
- Research risks and privacy risks are reasonable in relation to anticipated benefits;
- The organization has an adequate plan to protect identifiers from improper use or disclosure and an adequate plan to destroy identifiers at the earliest possible opportunity unless there is justification; and
- The organization has provided adequate written assurance that the protected health information will not be reused or disclosed.

"Researchers must provide documentation showing that the waiver was reviewed and approved by an internal review board in accordance with the common rule or by a privacy board," says King. "So if you don't have an IRB, you'll have to put together a privacy board."

Troubleshooting

HIPAA's privacy standards probably will also apply to areas that may not be immediately obvious, such as an organization's use of "shadow charts"—patient notes that are not an official part of the medical record.

"When you tell your doctors that they may not be able to keep those notes they've written on the backs of envelopes or cards or on sticky notes, you're going to get quite a reaction," notes King. "There'll have to be a lot of education about the ramifications of having private information on paper other than the medical record. The way you approach physicians on this will be key to getting their cooperation."

Other areas where healthcare organizations need to be careful:

- ***Medical record access:*** Organizations should have controls to limit employee access to the medical records of patients and other employees of the organization. "You need to assess whether people who have access to records really need to have it," says King.
- ***Computer access:*** Under HIPAA, healthcare organizations need to make sure patient medical information on computers is protected. King suggests setting up computers in a way that only the person authorized can see the computer screen when information is called up.
- ***Ancillary building communications:*** Look at how patient medical information is transported between different buildings in your organization, King suggests. "Do you just hand the chart to someone and say take it over? These are things we all need to work on correcting."
- ***Patient directories:*** Under HIPAA, organizations must inform patients that they may be listed in a patient directory and give them an opportunity to opt out. The listing itself may consist only of the name of the inpatient, general health status, and location.

Resource

- Carrie King: 713-794-4000

Separating The Wheat From The Chaff
How To Make Sure A Consultant Is Above Board

The HHS Inspector General's recent advisory bulletin on questionable practices of some healthcare consultants should help providers separate reputable advisors from unscrupulous ones, say consultants interviewed by *G-2 Compliance Report*.

The advisory bulletin warns healthcare providers to be wary of questionable practices, such as misleading representations about the consultant's relationship with the Medicare program, the Centers for Medicare & Medicaid Services (formerly HCFA) or the OIG; promising specific results that are unreasonable or improbable; encouraging abusive practices; or discouraging compliance efforts.

"A lot of what the OIG said was common sense, but it's a good reminder of things to watch out for," says Dane Cutler, president of Cornerstone Healthcare Services, a consulting firm based in Tampa, FL.

"Nothing the OIG says in it will hurt good consultants," adds Joan Logue, who is principal of Health Systems Concepts Inc. (Longwood, FL). "But I think there are a lot of consultants out there who are not well-informed, and providers should be careful whom they pick."

In particular, believes Cutler, providers should be leery of consultants who claim to have special connections at the OIG or to be endorsed by the OIG. "We all have contacts within different organizations. It doesn't mean we get special favors or privileges."

Both Cutler and Logue agree with the OIG's warning to be wary of consultants who promise a specific dollar or percentage increase in the client's Medicare reimbursement and base their fee on a percentage of the increased revenue.

Reputable consultants generally do not charge such "contingency fees," says Logue. "The OIG has made clear before that it frowns on contingency fees. Consultants should charge a flat rate for services."

Due Diligence

When hiring a consultant, Culter advises, providers should take a few simple steps to ensure the contractor is reputable:

1 *Involve counsel*. Ask your attorney to join you in meeting with the consultant and to review any contract before you sign. "I would be engaged through counsel, especially if the work involves compliance matters."

2 *Check references*. Talk to several other providers who have used the consultant's services. Often this is the best way to uncover an unscrupulous or incompetent one, notes Cutler.

3 *Examine the exclusions list*. Make sure the consultant is not excluded from participation in Medicare or Medicaid. The list is posted online at *www.hhs.gov/progorg/oig*. "I would look at the list before hiring someone and look at it again a couple of times a year," says Cutler.

Once you've hired a consultant, adds Logue, be sure that his/her recommendations are backed up by references to specific regulations or requirements. "Consultants who are giving bad advice cannot tie that advice to any regulations. In some cases you may want to look at the regulations and see how they apply to your specific situation."

Resources

- Dane Cutler: 813-975-1157
- Joan Logue: 407-774-5291
- Our previous coverage: "OIG, GAO Warn Providers Of Questionable Practices By Consultants," *Jun/Jul '01, p. 1*

Ohio Hospitals Settle Outpatient Lab Billing Suit

Ohio hospitals, satisfied they have changed the way the Federal Government pursues billing investigations, are preparing to dismiss a 1996 lawsuit that challenged what they call the government's "overly aggressive tactics," according to the Ohio Hospital Association (OHA).

OHA, along with the American Hospital Association, sued the Secretary of Health & Human Services five years ago to challenge investigations of outpatient lab billing, dubbed Operation Bad Bundle. Following an appeals court ruling that would have allowed the case to go to trial, OHA early this month reached a settlement agreement.

Under terms of the settlement, Ohio hospitals that had been required to file detailed annual compliance reports with the HHS Office of Inspector General will be relieved of that obligation.

The lawsuit was filed in October 1996 after several Ohio hospitals had been forced to settle allegations of overbilling Medicare and Medicaid because of the way bills for outpatient lab tests were presented to the government. A federal judge in Cleveland initially dismissed the suit on jurisdictional grounds, but the Sixth Circuit Court of Appeals in Cincinnati reinstated the lawsuit in December 1999 and ruled that hospitals may now go directly to federal court to challenge unfair Medicare billing rules.

COMPLIANCE PERSPECTIVES

Medicaid Enforcement Increasingly Sophisticated, Far-Reaching

Carolyn McElroy is of counsel with Mintz Levin Cohn Ferris Glovsky & Popeo, PC (Washington, DC). She is a former director of the Maryland Medicaid Fraud Control Unit and a former president of the National Association of Medicaid Fraud Control Units

When it comes to assessing regulatory risks in business decisions, the healthcare industry continues to monitor federally based enforcement initiatives closely, as well it should. But consider the following cases:

- A Washington State nursing home and its employees were convicted of submitting cost reports that billed the same care for the same dually-eligible patients to both Medicare and Medicaid.
- A national behavioral health provider serving the adolescent population paid $2.7 million to settle allegations that it billed "therapeutic leave" days—weekends and holidays when the teenage patients were permitted to visit their families—to Medicaid.
- A national pharmaceutical wholesaler paid $4 million and entered into a corporate integrity agreement to settle charges that its subsidiary "recycled" prescription drugs.
- The owners of several California laboratories were jailed and their assets confiscated after an investigation revealed they had masterminded a complex scheme to bill Medicare and Medicaid for millions for laboratory tests that were never performed—and for which they did not even have the necessary reagents.
- Three drug manufacturers were sued for allegedly defrauding the government by falsely overstating the estimated retail price of their drug products, thus causing the Medicaid program to set reimbursement higher than intended.

You might be surprised to learn that these significant healthcare prosecutions are *not* the work of federal enforcement agencies that garner daily attention from the industry press. Instead, they are the result of an increasingly productive and effective *state* healthcare enforcement team.

State agencies now call on multistate task forces of attorneys and investigators to attack complex antitrust, consumer protection, and false claims cases that, until a few years ago, were prosecuted only by federal agencies, if at all.

The federally funded state Medicaid Fraud Control Units, which have accounted for nearly 10,000 healthcare fraud prosecutions since their inception 25 years ago, have matured and are prosecuting increasingly sophisticated financial and quality-of-care fraud allegations.

So, what do *you* need to know about state enforcement efforts?

State Enforcement Agencies

The primary enforcement efforts for a state are often found in its Medicaid Fraud Control Unit. When the Federal Government established the Medicare program in 1965, it also passed legislation promising partial federal funding to states that adopted the companion program, Medicaid, designed by Congress to provide better healthcare coverage for the poor.

The Medicaid program provides matching federal funds at least equal to state expenditures for mandated and comprehensive healthcare coverage. States with a large number of citizens having below-average incomes may receive federal subsidies equal to three-fourths of their Medicaid program healthcare expenditures.

Unlike Medicare, however, Medicaid programs are administered by the states. This means that coverage, administration, regulatory enforcement, and fraud and abuse enforcement vary—sometimes widely—from state to state, except to the extent that federal regulations establish guidelines and standards that all state programs must meet in order to get federal funding. Fraud against the Medicaid program is, by virtue of its dual funding, punishable under both state and federal laws and may be prosecuted by either state or federal action.

Medicaid Fraud Control Units did not make their appearance until 1977, more than 10 years after the Medicare and Medicaid programs were established. The units were born after highly publicized fraud and abuse scandals caused Congress to realize that the honor

system didn't work, even where physicians were concerned, and no one was minding the store in either Medicare or Medicaid programs.[1] In rapid succession, Congress sought to stem fraud and abuse in both programs by offering block grant funding to state-based Medicaid Fraud Control Units in 1977, and by establishing the Offices of Inspector General (including the Departments of Health & Human Services and of Defense) in 1978.

Today, every state must have a federally subsidized Medicaid Fraud Control Unit (MFCU) unless it is able to show that program losses from fraud are *de minimis* because of existing state enforcement efforts or low Medicaid utilization. More than 2,000 persons are employed by MFCUs in 47 states and the District of Columbia,[2] and North Dakota may soon obtain approval for a unit.

In order to receive federal funding,[3] units must employ a "strike force" consisting of attorneys, investigators, and auditors dedicated solely to the prosecution of financial fraud by Medicaid providers (*e.g.,* filing false claims), patient neglect and abuse (failure to provide quality services), and fraud in administration of the program (*e.g.,* if a provider were to bribe a state official). The HHS Office of Inspector General (OIG) oversees MFCU funding and operations.

MFCUs are largely criminal enforcement units, though many have responded to the OIG's urging to undertake civil enforcement efforts as well. Some are sworn as police officers and are empowered to carry firearms, make arrests, and conduct search and seizure operations, while others emphasize accounting skills and healthcare expertise.[4]

In most states, attorneys for the MFCU are empowered to charge criminal and civil violations of law on their oath, while others are required to take their cases to local district attorneys or the U.S. Attorney's office for prosecution.

The manner in which MFCUs approach enforcement may be dependent on the unit's authority, composition, and the particular emphasis of the state's enforcement oversight. For a provider that becomes a target of a state investigation, the distinction may first be evident in the manner in which records are sought by the MFCU. Some units announce their presence with a search and seizure warrant; others have administrative summons powers that herald either a civil or criminal investigation. Still other states use the powers of the grand jury to compel testimony and the production of documents. The path, tenacity, and effectiveness of the prosecution effort will vary greatly from state to state. If confronted with a visit from the MFCU, you should hire an attorney who is—directly or indirectly—familiar with the individual units and how they approach the business of healthcare enforcement.

State enforcement efforts are, for the most part, contained within the Offices of the State Attorneys General. These Offices house 40 of the 47 MFCUs, which work side by side with antitrust, consumer protection, and insurance enforcement agencies. The Offices, working through the National Association of Attorneys General, have established a protocol for building multi-jurisdictional task forces to take on the tobacco industry, Microsoft, consumer fraud allegations, and allegations involving national healthcare issues.

Antitrust and consumer protection task forces have increasingly targeted healthcare cases involving allegations of misleading marketing, price-fixing, and retail pharmacy short-fills. Typically, a provider seeking to settle a multi-state case will face a task force made up of some (but perhaps not all) of the states in which the provider does business.[5]

Coordinated Prosecutions

Though it was perhaps once true that "the right hand didn't know what the left hand was doing" when it came to federal and state enforcement efforts, these efforts today are generally well coordinated. The states often informally share information on investigations with their federal counterparts.

MFCUs are required to file formal quarterly and annual reports summarizing cases, investigations, and convictions; to report convictions to the federally maintained database of healthcare convictions and settlements; and to report all healthcare-related convictions to the OIG so that it may exclude providers where appropriate.

Providers are likely to find highly effective cooperation between state and federal governments in the following instances:

❖ **Joint investigations** involving both federal and state personnel. These are likely in cases where the governments suspect that Medicare, Medicaid, and privately insured patients have been defrauded. The joint investigation may be initiated

[1] The Bureau of Health Insurance (later HCFA; CMS) did not have any programs designed to identify possibly fraudulent Medicare billings. And, though Congress had assumed that the states would enforce against Medicaid fraud, it had failed to realize that the states did not want to invest large sums in prosecuting complex healthcare cases when most of the amounts lost or recovered were federal funds.

[2] North Dakota, Idaho, and Nebraska are the states without MFCUs.

[3] Federal funding is 90% for the first three years of a MFCU's life, and 75% thereafter.

[4] The units may not be housed in the same agency as the Medicaid program administration, per federal regulation.

[5] When settling such cases, care must be taken to evaluate the contingent liabilities presented by the 'excluded' entities.

by either the state or the federal government, meaning that a knock on the door by one means that issues relating to all payers[6] should be evaluated for potential problems.

❖ **Global settlements** of national cases involving both Medicaid and Medicare issues. When the Department of Justice investigates potential Medicaid violations, it often looks to the MFCUs to collect information on state damages and to assist in settling state Medicaid issues. The first of these so-called "global" cases was the 1992 settlement with National Health Laboratories. MFCUs have participated in the investigation and settlement of most national healthcare cases since, facilitating settlements between the defendants and the involved states.

❖ ***Qui tam* suits**. Historically the sole province of federal healthcare fraud enforcement, these cases have expanded into the state arena now that more than a dozen states have passed whistleblower statutes. Savvy whistleblowers' counsel typically file copycat suits at both federal and state levels so they can increase their chances of intervention and collect whistleblower fees from both the federal and the state Medicaid damages.[7]

❖ **Sting operations**. Task forces may, for example, set up bogus storefront clinical operations to trap unwary ancillary service providers into offering or soliciting kickbacks. The sting operations generally involve video cameras and tape recorders.

❖ **Steering committees**. These and other variously named federal and state law enforcement meetings are held to share information on ongoing cases and allegations.

❖ **Corporate Integrity Agreements**. CIA enforcement is a shared concern between state and federal governments. Federal CIAs are often negotiated with both state and federal interests in mind, and the states may call on the OIG if they uncover billing problems with a provider operating under a CIA. Thus, a provider operating under a federal CIA must be equally careful that state operational issues are dealt with appropriately.

❖ **Data sharing**. This is last, but not least, on the list of state and federal co-operation. The states are required to provide information to the Federal Government for its investigations upon request, and in most states requests for information are filtered through or communicated to the MFCU.

Protecting Yourself

If confronted by a state enforcement agency, the most important rule is to get counsel immediately. Anything you say and do in an enforcement action is the functional equivalent of walking in wet concrete. If you don't know the focus of the state's activity, or don't understand all of the law involved, you may leave permanent footprints that head in the wrong direction.

First, it is important to identify with whom you are dealing. Know the state agencies that enforce allegations of healthcare fraud in the state(s) where you operate, and be sure that key personnel recognize the agencies by name. Be aware that, in some cases, regulatory individuals (licensing and certification, for example) show up for routine reviews with an enforcement agency tag-along.

Second, apply all of the general rules you would use if contacted by a federal healthcare enforcement agency. Don't submit to an interview or turn over records without service of adequate process and consultation with *healthcare litigation* counsel. Don't assume that the state will be a lesser threat than the federal enforcement agency. States may have differing laws, different priorities, or lower prosecution thresholds. States have literally prosecuted cases involving individual claims of less than $100 in fraud when it fit a state prosecution agenda.

Third, assume that every question will be a trick question, and nothing is off the record. For this reason, it is important to decline, repeatedly and politely, to answer any questions posed by the agent. Assume also that everything you say will be heard by all other state and federal enforcement and regulatory agencies. For example, don't assert that a discrepancy in a state claim is due to a particular federal 'technicality' because the state probably has already spoken with federal authorities—or will as soon as they leave.

Fourth, make sure you know the state law. It may differ significantly from the federal law. For example, many states have anti-kickback statutes that mirror the federal law, but don't have the corresponding federal safe harbors. Others have unexpected exclusion and penalty clauses that kick in once you settle.

Finally, make sure you consider the collateral issues before deciding what to do. If you have engaged in similar practices in 30 states, settling in one will not make a problem "go away." Most states have ironclad sunshine polices and will issue a press release that will bring the other 29 states to your doorstep after the settlement (if they are not already there.)

❖ *Ms. McElroy may be reached at Mintz Levin, 701 Pennsylvania Ave. NW, Washington DC 20004. Tel: 202-434-7408. E-mail: cjmcelroy@mintz.com*

---

[6] HIPAA gave federal enforcement authorities the right to prosecute private insurance healthcare fraud—a right they arguably always had by use of mail and wire fraud statutes.

[7] The federal False Claims Act is widely read as permitting a whistleblower to collect a percentage of only those funds that are federally subsidized. Whistleblowers do not collect money for recoveries of state-funded damages in the absence of a corresponding state false claims statute.

Standard Medicare ABNs Approved, CMS Working on Instructions

The Office of Management & Budget has approved a new uniform, single-page format for the Advance Beneficiary Notice (ABN) used to obtain consent from Medicare beneficiaries before billing them for Part B items/services that Medicare will not pay for.

One ABN is designed especially for laboratory services (Form CMS-R-131-L, *see below*); another (CMS-R-131-G) is for general use. (Beneficiaries receiving Part A services get inpatient notices of non-coverage, instead of ABNs.)

The final version of the ABNs is similar to previous drafts, but does include new language to address physician concerns. Dropped is terminology like "not medically necessary" that could confuse beneficiaries. Instead, there is a new explanation that Medicare does not pay for all tests and services. "The fact that Medicare may not pay for a particular item or service does not mean you should not receive it," the notice says. "There may be a good reason your doctor recommended it."

According to officials at the Centers for Medicare & Medicare Services (CMS), providers/supplier may preprint their own forms, with check-offs for reasons for coverage denials common to their business, as long as the format and readability of the ABNs are maintained. Any preprinting, however, must be in at least 12 point Arial or Arial Narrow or a similarly readable font.

Patient's Name: Medicare # (HICN):

ADVANCE BENEFICIARY NOTICE (ABN)

NOTE: You need to make a choice about receiving these laboratory tests.

We expect that Medicare will not pay for the laboratory test(s) that are described below. Medicare does not pay for all of your health care costs. Medicare only pays for covered items and services when Medicare rules are met. The fact that Medicare may not pay for a particular item or service does not mean that you should not receive it. There may be a good reason your doctor recommended it. Right now, in your case, Medicare probably will not pay for the laboratory test(s) indicated below for the following reasons:

Medicare does not pay for these tests for your condition	Medicare does not pay for these tests as often as this (denied as too frequent)	Medicare does not pay for experimental or research use tests

The purpose of this form is to help you make an informed choice about whether or not you want to receive these laboratory tests, knowing that you might have to pay for them yourself. Before you make a decision about your options, you should read this entire notice carefully.

- Ask us to explain, if you don't understand why Medicare probably won't pay.
- Ask us how much these laboratory tests will cost you (Estimated Cost: $_____), in case you have to pay for them yourself or through other insurance.

PLEASE CHOOSE ONE OPTION. CHECK ONE BOX. SIGN & DATE YOUR CHOICE.

☐ Option 1. YES. I want to receive these laboratory tests.
I understand that Medicare will not decide whether to pay unless I receive these laboratory tests. Please submit my claim to Medicare. I understand that you may bill me for laboratory tests and that I may have to pay the bill while Medicare is making its decision.
If Medicare does pay, you will refund to me any payments I made to you that are due to me.
If Medicare denies payment, I agree to be personally and fully responsible for payment. That is, I will pay personally, either out of pocket or through any other insurance that I have.
I understand I can appeal Medicare's decision.

☐ Option 2. NO. I have decided not to receive these laboratory tests.
I will not receive these laboratory tests. I understand that you will not be able to submit a claim to Medicare and that I will not be able to appeal your opinion that Medicare won't pay.
I will notify my doctor who ordered these laboratory tests that I did not receive them.

Date _____ Signature of patient or person acting on patient's behalf _____

NOTE: Your health information will be kept confidential. Any information that we collect about you on this form will be kept confidential in our offices. If a claim is submitted to Medicare, your health information on this form may be shared with Medicare. Your health information which Medicare sees will be kept confidential by Medicare.

OMB Approval No. 0938-0566 Form No. CMS-R-131-L (June 2001)

Labs and physicians may begin using the ABNs now, but will not required to adopt them until the implementing instructions for carriers and intermediaries are completed, probably sometime this fall, said Raymond Boyd of the CMS Center for Beneficiary Choices at a briefing of the Practicing Physicians Advisory Council.

According to Boyd, CMS is working on a separate beneficiary brochure explaining statutory exclusions from Medicare benefits, financial liability rights, and appeal rights. The brochure should be completed next year, he said.

The new ABN forms are expected to be downloadable from the CMS Website (*www.hcfa.gov*) in the near future.

Resource

❖ Raymond Boyd: 410-786-4544

Is Voluntary Disclosure A Good Idea? It All Depends

In a recent report, the HHS Office of Inspector General says healthcare providers that voluntarily disclose misconduct to the government are more likely to receive more lenient treatment than those who don't.

But outside attorneys say providers should think carefully before automatically disclosing problems.

The OIG's Report

The OIG, as part of its ongoing self-assessment of healthcare compliance initiatives, conducted an informal survey of the results of corporate integrity agreement (CIA) negotiations since then-Inspector General June Gibbs Brown issued her "Open Letter to Healthcare Providers" in March 2000.

The purpose of the review was to determine the extent to which providers' existing compliance efforts and self-disclosure of misconduct influenced the decision to require a CIA or modify specific terms.

In general, the survey found that when the OIG believed a CIA was necessary and when there was objective evidence of a comprehensive compliance program, the OIG often made two significant modifications to the CIA:

- A reduction in its term from the usual five-year time period to three years.
- A reduction in the role of the independent review organization in those cases where the provider could demonstrate that it had an established system of internal audits.

"These two modifications alone represent a significant benefit to the provider," says the OIG. "Other modifications generally focused on conforming the requirements of the CIA to the provider's existing compliance infrastructure. These modifications … were intended to promote continuity in the provider's ongoing compliance program."

Assess Each Case Separately

Although the OIG may go a little easier on providers that voluntary disclose misconduct, self-disclosure of problems may not always be advisable, believes attorney Brad Tully of Los Angeles-based Hooper Lundy & Bookman.

"The OIG says it doesn't negotiate, but that's not true," Tully says. "In many cases, a provider can actually negotiate a better deal than the one the OIG offers in return for self-disclosure."

Tully advises providers to assess each case separately and consult with their attorneys before automatically disclosing any type of problems that could be perceived as misconduct.

Craig Holden, a shareholder with the law firm of Ober/Kaler (Baltimore, MD) agrees that providers must think carefully before disclosing information that could be used against them, but warns against withholding certain kinds of information, particularly if an overpayment is involved.

"Knowing of a problem and not disclosing [it] may even create additional liability or even potential criminal liability," he says. In general, a provider reports mistakes resulting in overpayment to its fiscal intermediary or carrier, which then would decide whether to report that information to the OIG.

While Holden believes providers that voluntarily report problems may actually receive some leniency from the OIG, he also believes there should be even more incentives for providers to come forward with oversights or mistakes.

"Having to hire someone to do the kind of audits some of the CIAs require can be very expensive," he says. "Is it a break not to have to do that? Absolutely. Is it a break if a CIA lasts for three years, not five? Absolutely. But I think providers making those kinds of disclosures would view imposition of a three-year CIA as incredibly onerous. It's sort of like the old adage that no good deed goes unpunished."

Resource

- OIG: "Self-Disclosure Of Provider Misconduct: Assessment Of CIA Modifications," *www.hhs.gov/progorg/oig/cia/assessment.htm.*
- Brad Tully: 310-551-8111
- Craig Holden: 410-347-7322

OIG Touts Benefits Of Self-Disclosure

The HHS Office of Inspector General offers a number of examples of modifications made to corporate integrity agreements (CIAs), based on providers' voluntary self-disclosure of misconduct, including the following:

- A rural hospital in the Southeast self-reported that, while under former ownership and management, it had submitted claims with information that was falsified to support reimbursement. The hospital uncovered the false claims during an internal audit performed as part of its voluntary compliance program. In the fall of 2000, the hospital agreed to resolve its financial and exclusion liability. The OIG did not impose a CIA because the misconduct was committed by the former management and the new management disclosed its findings to the government as part of a comprehensive pre-existing compliance program.
- A network of physician clinics in the Northeast agreed in the spring of 2000 to resolve its False Claims Act liability arising from submission of claims that violated Medicare's "incident to" billing rules. The OIG imposed a five-year CIA on the network; however, the integrity obligations were tailored to the providers' pre-existing compliance program. Moreover, the physician clinics were allowed to qualify for internal annual reviews, instead of reviews by an independent review organization.

Govt. Isn't Targeting Inadvertent Errors, Says OIG Attorney

Contrary to what many in the healthcare industry might believe, federal prosecutors are not targeting physicians, laboratories, or hospitals for technical or inadvertent mistakes in filing Medicare and Medicaid claims, says an official with the HHS Office of Inspector General.

Clear and blatant violations of the law are the prime concern, not simple mistakes or billing errors, senior OIG attorney Gary Thompson tells *G-2 Compliance Report*.

"The government doesn't target honest billing errors for criminal and civil prosecution. We want to dispel the myth that we're somehow going after providers for little things. The reality of what we're doing dispels that."

At the broadest level, the government's approach to investigations is similar for physicians, hospitals, and labs, Thompson says. "When a hospital or lab is analyzed in terms of what kind of compliance program it has, it's the same broad concept that we're focused on, though the analysis might differ slightly depending on the exact circumstances of the case."

Factors At Play

In probing whether billing errors result from a simple mistake or represent a pattern of duplicity, federal investigators consider a number of factors, including whether a provider has a compliance program in place, notes Thompson.

"If a defendant in a civil False Claims Act case comes to us or to the Justice Department and says, 'Don't find me liable under the Act because I've got this crackerjack compliance program,' we're going to look behind what's on paper. Obviously, what's on paper is very important, but we'll also look to see if the policies and procedures are being implemented."

The OIG will look in particular, Thompson says, at whether the seven basic elements of a compliance program are in place: written policies and procedures; designation of a compliance officer and/or committee; education and training programs; communications between the compliance officer and employees; discipline for failure to adhere to compliance policies and procedures; ongoing auditing and monitoring; and reporting of suspected non-compliance.

Of some 474 corporate integrity agreements (CIAs) in effect with healthcare providers, according to Thompson, 300 are with hospitals, 75 with practitioners, 15 with nursing homes, 12 with pharmacies, and 10 each are with laboratories and outpatient clinics. The OIG also is monitoring a few CIAs with home health agencies, billing contractors, mental health providers, and managed care organizations.

Resource

❖ Gary Thompson: 202-619-3148

Physicians Snared, *from page 1*

is certainly more suitable than criminal prosecution. Prior to 1997, criminal prosecution was the only choice."

The Balanced Budget Act of 1997 authorized the OIG to impose CMPs of up to $50,000 per kickback offered, paid, or received, plus triple damages.

Operation Takeback

The settlements with the Florida physicians are the result of an investigation into Clearwater Clinical Laboratory and Community Clinical Lab that began in 1996 and was part of a larger operation called "Operation Takeback." That investigation, led by Gary Montilla, the former assistant U.S. attorney for the Middle District of Florida, allegedly turned up the names of hundreds of doctors who had received kickbacks, say sources.

The labs, their owners, and the general manager pled guilty last year to one count each of conspiracy to defraud the government and five counts of kickbacks to four doctors. James L. McKeown Jr., the minority owner of CCL, was sentenced to six months in a halfway house earlier this year. His father and CCL majority owner, James L. McKeown, and CCL's general manager, Vincent Gepp, were sentenced to three years' probation.

As of April 2001, 14 physicians had been indicted for their business dealings with CCL, according to Kenneth Webster, executive director of the Pinellas County Osteopathic Medical Society. Two of them, Michael Spuza and Ira Havey Liss, were found guilty by a jury in April. Liss was sentenced to 15 months in jail and ordered to pay $34,600 in restitution. Spuza was sentenced to 18 months in jail and ordered to pay $55,371 in restitution. Both convictions and sentences are currently on appeal.

Charges against one of the 14 physicians were dropped, according to Webster. The other physicians agreed to plea bargains, received 1-3 years' probation, paid a fine, and lost their ability to participate in Medicare for up to five years, he says. There have been no further criminal indictments since July 2000.

The Florida physicians involved in the recent civil settlements, as well as those involved in the earlier indictments, allegedly accepted kickbacks from Clearwater Clinical Laboratory; another lab, SOMED

Co.; and various other diagnostic centers from 1992 to 1998 in exchange for patient referrals. The alleged kickbacks included companies paying physicians higher than market-value monthly rent for space in their offices and paying for physician office staff or phony consulting work.

According to Webster, the recent civil settlements represent a new, gentler approach to punishing the physicians alleged to have received kickbacks. Montilla, who has since left the U.S. attorney's office, pursued criminal indictments aggressively while in office, says Webster. "Now that he's gone, it's calmed down a lot. We wanted civil settlements for all of the physicians all along."

The five Florida physicians who settled included Mohammed Kadiwala, MD; Nickolas John Colluci, DO; Hugo Scavino, MD; Elbert Barnes, MD; and Joseph Fortunato, MD. Several entered into five-year integrity agreements with the OIG. The sixth settlement was reached with New York physician Jai Rhee, MD, who signed a three-year integrity agreement.

All of the doctors denied any wrongdoing. CMPs imposed on the group ranged from $16,500 to $150,000.

Wake-Up Call

The Clearwater investigation and resulting settlements have had a sobering impact on physicians in the Tampa Bay area, according to Imperato, who advises physicians to become more knowledgeable about the anti-kickback statute.

"If physicians haven't taken notice of culpability under the statute up till now, they certainly should from here on. Ignorance of the law is not necessarily going to be a good defense in a kickback case. Physicians should get competent advice about any financial relationships they have with an entity that is a source of referrals or to which they refer."

Now that the government has imposed civil fines against physicians in kickback cases, it's likely that more will be brought throughout the country, Imperato believes. Along with the civil penalties, the government may exclude providers from participation in Medicare and Medicaid.

"The remedies are still quite serious, even if they aren't criminal," he says.

Prosecutor's Overreach?

The Pinellas County Osteopathic Medical Society, which has accused Montilla of "prosecutorial overreaching," plans to file a "prosecutorial misbehavior" case against the former prosecutor in an attempt to have the criminal indictments overturned.

"These should not be felonies when these people had no idea they had done anything wrong," says Webster. "We don't believe the indictments were fair. We're satisfied with the civil settlements."

While Montilla reportedly told defense lawyers that he expected 100 convictions, there have been no further indictments since he left office, Webster says. "We think, we feel that the investigation has been stopped."

Steve Cole, a spokesman for the U.S. attorney's office, declined to say whether the investigation was continuing or whether additional settlements or indictments are expected.

Resources

- HHS Office of Inspector General: 202-619-3148
- Gabriel Imperato: 954-764-7060
- Steve Cole: 813-274-6100
- Kenneth Webster: 727-581-9069
- Our previous coverage: *May '00, p. 12; Jun/Jul '99, p. 12*

The Benefits Improvement & Protection Act of 2000 included a "grandfather" provision that allows independent laboratories to continue billing Medicare directly for the technical component (TC) of pathology services to hospital inpatients and outpatients through 2002, as long as those arrangements were in place with a hospital on or before July 22, 1999. To qualify, must hospitals maintain such arrangements with these labs? What if a hospital decides to switch labs?

The grandfather provision applies to the hospital, not the lab, according to a recent program memo from the Centers for Medicare & Medicaid Services (Transmittal AB-01-47).

A "covered" hospital, the memo says, is one that had an arrangement with an independent lab in effect as of July 22, 1999, under which the lab furnished the pathology service TC to fee-for-service Medicare beneficiaries who were hospital inpatients or outpatients and submitted claims for payment for the TC to a carrier. The TC could have been submitted separately or combined with the professional component and billed globally.

"If a hospital is a covered hospital, *any independent laboratory* that furnishes the TC of physician pathology services to that hospital's inpatients or outpatients can bill the carrier for these services furnished in 2001 and 2002," says the memo (*emphasis added*).

Transmittal AB-01-47 is posted online at *www.hcfa.gov/pubforms/transmit/AB0147.pdf*.

Have a question you'd like answered? Please e-mail to Kimberly Scott, editor, at *kimscott@yahoo.com*. We'll select one to address in this column.

The Back Page

News-At-A-Glance

Double Billing Debacle: Humana Medical Plan Inc. (Louisville, KY) will pay nearly $8 million to settle allegations that it billed both Medicaid and Medicare for the same capitated services, according to Florida Attorney General Robert Butterworth. Humana has agreed to revise its billing procedures to prevent further occurrences. The case involved Medicaid recipients who were dually enrolled in Medicaid and Medicare managed care plans operated by Physicians Corp. of America (PCA) between July 1, 1992 and Dec. 31, 2000. Humana discovered the billing problems shortly after purchasing PCA in 1997, according to a spokesman. Humana will pay back all funds improperly collected, as well as cover the cost of the state's investigation.

DME Downfall: American HomePatient Inc. and affiliate American HomePatient Delaware (collectively, AHOM, based in Brentwood, TN) have agreed to pay $7 million to resolve false claim allegations that AHOM, which provides medical equipment and home infusion supplies, submitted claims for payment based on inadequate supporting documentation or stemming from illegal patient referrals to several federal programs. Former employee Kenneth Hollis, who raised the allegations, will receive $1.17 million as part of the settlement.

Fraudulent Admissions: East Texas Medical Center (Jacksonville) will pay $1.5 million to settle allegations that it defrauded Medicare by unnecessarily admitting patients, according to the HHS OIG. Federal officials charged that East Texas and two local doctors profited by billing Medicare for fraudulent admissions between April 1995 and December 1996. The two doctors, Gregory Kotheimer and Romeo Guillermo, settled allegations against them in June and agreed to permanent exclusion from Medicare and Medicaid. The hospital has signed a five-year corporate integrity agreement.

Reprocessed Single-Use Devices: The Food & Drug Administration has produced two documents to help hospitals and other healthcare facilities comply with its recent directive on reprocessing single-use devices for patient care (*G-2 Compliance Report, May '01, p. 1*). The latest issue of the User Facility Reporting Bulletin gives an overview of each regulatory requirement (online at *www.fda.gov/cdrh/fusenews/ufb34.htm*). The Frequently Asked Questions page on the Reuse Website has been updated with guidance on sterilization and hospital management responsibilities (*www.fda.gov/cdrh/reuse/reuse-faq.shtml*).

Waived Labs Score Badly: The basic regulatory requirement for CLIA waived testing is "follow the manufacturer's instructions." But a nationwide survey by the Center for Medicare & Medicaid Services has found that 32% of CLIA-waived labs failed to have current instructions for their testing, 16% didn't follow instructions, 9% didn't follow storage and handling instructions, and 6% were using expired reagents and kits. The preliminary findings, based on a CMS study from October 2000 to January 2001, showed that 48% of all waived labs surveyed had quality testing problems.

G-2 Compliance Report (ISSN 1524-0304). © 2001 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.