COMPLIANCE HOTLINE™

THE NATION'S ESSENTIAL ALERT FOR HEALTHCARE COMPLIANCE OFFICERS

MONDAY
NOVEMBER 16, 1998

New government data bank will register all 'adverse actions' against providers

Offenders list to include sanctioned physicians

If the OIG gets its way, a new federal database will register all so-called adverse actions taken against providers — even if those actions are still under appeal.

The Healthcare Integrity and Protection Data Bank (HIPDB), mandated by the HIPAA legislation, is intended to be a register of any adverse actions against providers, such as civil or criminal judgments or convictions, licensing actions, and exclusions. It would include actions that involve unsound fiscal, business or medical practices that cost Medicare money, don't meet accepted standards of care or affect patient care.

That's straightforward enough, and few people are likely to challenge the concept of a system to track repeat offenders. But the fact that adverse actions still under appeal by physicians, hospitals and other providers must also be submitted troubles **Pat Smith**, director of governmental relations for the Englewood, CO-based Medical Group Management Association. "It raises a basic question of fairness," Smith adds. It also troubles a compliance officer at a large university group practice in the Southwest. "If it's unresolved, how can it go into a data bank?" asks the compliance officer, who asked for anonymity.

Another rub lies in a provision of HIPAA that gives HHS the discretion to include other types of adverse actions. OIG believes Congress "intended a broad interpretation of the terms 'health care fraud and abuse,'" according to the proposal. And the agency is choosing to define adverse actions

*See **Data bank**, page 2*

HCFA to PROs: Cut billing errors at least 10%

Peer review organizations (PROs) may be the government's newest allies in its war on health fraud. HCFA's new statement of work for PROs tasks them with detecting billing errors and reporting errors to OIG and other enforcement agencies.

More ominous is a HCFA directive that PROs must actively reduce billing errors. Each PRO will be expected to cut errors at least 10% during the three-year contract, with HCFA's ultimate goal for the entire program to slash total errors by half.

*See **PROs**, page 4*

Search warrant: What to do when feds come knocking

The agents are knocking at your door, badges are flashing in your face, and you've just been handed a search warrant. Even if you didn't do anything wrong, they think you did, and they intend to check you from top to bottom.

As the raids on Nashville, TN-based Columbia/HCA over the past year have shown, this is not a paranoid scenario. And if a search does happen, it is definitely not a time when you want to improvise. You need your managers and employees to understand what they should — and should not — do if the worst happens and the FBI shows up with a warrant. Here are some quick do's and don'ts on handling a search from **Amanda Mott**, JD, an attorney with von Briesen, Purtell & Roper, in Milwaukee.

DO:

♦ Ask the investigators to wait until the employee-in-charge arrives. This employee could be the

*See **Search warrant**, page 2*

Data bank

Continued from page 1

to include administrative decisions by health plans, such as depriving a practitioner of clinical privileges.

Hold on, says **Bill Mahan**, executive director of the National Healthcare Anti-Fraud Association, which represents private insurers and HMOs. No health plan on earth is going to restrict a physician and publicly admit it's because of concerns about fraud. That's an open invitation for a lawsuit. Health plans dread finding themselves caught between the proposed $25,000 per day fine for not reporting adverse actions and a multimillion-dollar lawsuit from an outraged physician, Mahan says.

In addition, the current crusade against health fraud makes it easy for a provider to get a black mark, worries the Southwestern compliance officer. "The ability to accuse someone in a group practice or hospital setting is very easy if there's a simple mistake that ends up costing millions," she adds.

Other facets of the proposed regs, which are open for public comment until Dec. 29, include:

- Those having to report adverse actions and those having access to the database include HMOs, private insurers, and government agencies.
- Providers whose actions must be reported to the data bank include physicians, nurses, chiropractors, podiatrists, emergency medical technicians, physical therapists, pharmacists, clinical psychologists, acupuncturists, dietitians, aides, and licensed or certified alternative medicine practitioners such as homeopaths and naturopaths.
- Those who submit reports to the HIPDB won't be liable for their accuracy unless they actually knew them to be false. Federal and state agencies must submit reports to the data bank either within 30 days of the adverse action or when the agency knew the adverse action was taken.
- Agencies and health plans would have to collect Social Security and Employer Identification numbers for purposes of reporting to the HIPDB.
- Doctors won't be able to evade the system by voluntarily surrendering, or not renewing, their licenses before they are sanctioned. Any provider under investigation, or who surrenders a license to settle a probe, will be reported to the HIPDB.
- OIG wants reporting to include any adjudicated action, such as orders by an administrative law judge, civil monetary penalties and assessments, revocations, debarments, and loss of clinical and staff privileges at a health plan.
- Anyone accessing the data bank would pay a fee, though the subject of each report to HIPDB gets a free copy. HIPDB records may only be accessed for purposes of preventing health fraud and improving patient care. For privacy reasons, the data bank won't contain any individually identifiable patient records.
- Providers can dispute the accuracy of a report to the NIPDB, though they can't dispute the underlying judgment that fueled the report.
- The program will be phased in gradually, beginning with licensure actions, federal criminal convictions and civil judgments, and exclusions. ■

Search warrant

Continued from page 1

compliance officer, the provider's counsel, an on-call administrator, or the CFO. He or she will be the one to negotiate with the agents.

- Request copies of the warrant and the affidavit providing reasons for why the warrant was issued.
- Ask for an opportunity to confer with counsel before the search commences. If your attorney can be reached by phone, put him or her directly in touch with the lead investigator.

Continued on page 3

Compliance Hotline® is published every two weeks by American Health Consultants®, 3525 Piedmont Road, Building Six, Suite 400, Atlanta, GA 30305. Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. *Compliance Hotline*® is a trademark of American Health Consultants®, a Medical Economics Company.

SUBSCRIBER INFORMATION
Please call **(800) 688-2421** to subscribe or if you have fax transmission problems. Outside U.S. and Canada, call **(404) 262-5536**. Our customer service hours are 8:30 a.m. to 6:00 p.m. EST.

Search warrant

Continued from page 2

♦ Cooperate with the investigators, but do not consent to the search. The employee-in-charge should inform the lead investigator that the provider objects to the search because the search will violate the rights of the provider and its employees.

♦ If you can't reach counsel, contact the prosecutor handling the case and ask that the search be stopped. Try to negotiate alternatives, such as ensuring that evidence will be left undisturbed. If the prosecutor won't stop the search, ask him to delay it until you can get a court hearing.

♦ Negotiate an acceptable methodology with the investigators to minimize disruptions and keep track of the process. This can cover the sequence of the search, whether copies can substitute for originals, and whether you'll have access to seized records. Disputes regarding the scope must be brought to the attention of the prosecutor or the court to be settled. No one should attempt to prevent investigators from searching areas they claim to have the right to search.

(Remember that federal investigators generally have the right to seize evidence of crimes that is in their "plain view" during a search regardless of whether such evidence is described in the warrant.)

♦ Keep track of all documents given to investigators as well as the information they contain.

♦ Make sure that employees understand that they don't have to speak to the investigators, but must provide the documents requested in the warrant.

♦ Send all but essential personnel home, or temporarily reassign them to other areas.

♦ Designate selected employees to remain with the employee-in-charge to monitor the search. Investigators should never be left alone on the premises, and no employee should be left alone with the investigators. Several individuals will be probably be needed to monitor the different areas being searched simultaneously.

If a monitor is ordered to leave, contact the lead investigator. A person should be ordered to move only if he or she is in the way, but not because agents want to conduct their search unobserved.

♦ Object to any search of privileged documents. Try to negotiate a methodology to protect the confidentiality of any privileged information pending a resolution of these objections. For example, you might segregate the privileged documents from other files and put them in sealed envelopes, which agents won't open and read until a court has decided the matter.

♦ Keep a record regarding the search. Ask each investigator for proper identification, including their business cards. List the names and positions of all the investigators with the date and time. Verify the list with the lead agent and request he or she sign it. Monitor and record the manner in which the search is conducted. Note in detail the precise areas and files searched, the time periods when each of them was searched, the manner in which the search was conducted, the agents who participated, and which files were seized.

♦ If possible, videotape the search. If the investigators claim the taping interferes with the search, the employee-in-charge should make a record of the refusal. Do not persist if the agents have warned that they regard the taping as an interference.

♦ If possible, make a record and a copy of all records seized. If this is not possible, before the agents leave the premises, request an inventory of the documents seized. Download copies of files from hard drives of computers, and copy diskettes, especially if the material is essential to your ongoing operations.

DON'T:

♦ Alter, remove, or destroy permanent documents or records. In fact, once you're aware of an investigation, even routine destruction of records must stop.

♦ Obstruct or interfere with the search. But while they should cooperate, employees should also clearly state that this does not constitute consent to the search.

♦ Consent to an expansion of the search. The employee-in-charge should point out limitations on the premises to be searched and on the property to be seized. Avoid expansion beyond the proper scope of the search from confusion or overreaching. ■

DOJ to put private payers on regional task forces

Expect more aggressive fraud enforcement in the wake of new guidelines issued by Attorney General Janet Reno.

The guidelines create a formal structure for cooperation between the Justice Department and private insurers. This marks a sea change for insurers who were never sure how much cooperation they could expect from each individual US Attorney, says **Bill Mahan**, executive director of the National Healthcare Anti-Fraud Association, which represents the fraud units of insurers and HMOs. For example, a regional fraud task force run by DOJ might eschew private payer fraud in favor of concentrating on Medicare and Medicaid fraud.

Now the government will put insurers on the regional task forces. More important, the Justice Department will appoint "information exchange coordinators," and expects insurers to do the same. DOJ wants insurers to turn over information on health fraud, as well as any useful resources that private fraud control units use.

In return, the Department of Justice pledges to turn over information on specific frauds to the particular insurers affected by those crimes, as long as the distribution is "practicable, permitted by law, and will not jeopardize ongoing law enforcement investigations."

More specifically, the department will disseminate public information such as settlements and indictments. In addition, there will be periodic newsletters that will discuss enforcement actions, as well as copies of reports submitted to the new Healthcare Integrity and Protection Data Bank.

As for the trickier matter of non-public information that the government uncovers, DOJ says it will try to provide what data it can. If health plans alert investigators to fraud committed by a provider, DOJ says it will try to keep the insurer abreast of the scope of the fraud and the outcome of the investigation.

It also promises to keep confidential the sources of the insurer's information. That will soothe an insurer's worst nightmare, says Mahan: That it passes on information on a fraud scheme, only to see the local US Attorney lay down indictments just for Medicare and Medicaid, and then collect a big settlement that doesn't recoup money lost by the insurer.

Now DOJ says it will try to provide information that will let insurers get restitution, including money and property seized by the government. And if a private insurer is sued for turning information over to federal investigators, the Justice Department will provide affidavits defending the insurer's action, says Mahan. ■

PROs

Continued from page 1

Their reward will be a hefty bonus that pays .05% of their base contract for every 1% that errors drop in their states, to a maximum of 10%. PROs that discover fraud must refer the cases to fiscal intermediaries or enforcement agencies like OIG.

This could poison the relationship between providers and PROs. Providers groups have already indicated that they expect their members to be less cooperative with PROs, says **Regina Buchanan**, director of quality improvement for the American Health Quality Association, which represents PROs.

HCFA will judge PROs on their success in implementing a Payment Error Prevention program, which is designed to spot inpatient PPS errors. This includes "pattern analysis of billing data and individual record reviews," according to HCFA. HCFA also expects PROs in each state to identify trends, such as incorrect DRG coding, inappropriate transfers, premature discharges and medically unnecessary care. Those trends will be used to create new areas for PROs to focus on. Buchanan says the details have yet to be worked out, but the system may involve HCFA identifying large-scale patterns of coding errors, then asking PROs to spot providers who fall outside baseline norms. Note: the statement of work specifically directs PROs to initially focus on reviewing and reducing the number of unnecessary hospital admissions and the number of DRG upcodings.

In the past, HCFA referred records of cases involving suspected fraud to PROs for analysis. HCFA later shifted the focus of PROs to quality of care, and now fraud is getting a major issue in peer review. PROs will be asking HCFA to ease some of the fraud review requirements, which essentially put PROs in the uncomfortable role of behaving like fiscal intermediaries, says Buchanan. ■