

Radiology Administrator's

Compliance & Reimbursement Insider

FEBRUARY 2002

Take Nine Security Measures When Employee Quits or Is Fired 1

Include these security measures in your employee termination procedures to protect yourself from security breaches and move toward HIPAA compliance.

- ▶ Model Checklist: Track Security Measures Taken When Employee Leaves (p. 3)

How to Avoid Trouble as Insurers Target 'Over-Reads' 4

Medically necessary over-reads help improve patient care, but billing for unnecessary over-reads can land your practice in hot water.

Ask the Insider 6

- ▶ Hospital-Based Practice May Bill Globally in Certain Circumstances
- ▶ Billing for Mammogram of Patient with Breast Implants in Absence of Signs or Symptoms

Protect Yourself from Inaccurate Data Bank Reports 7

Your data bank report can have a huge impact on your career—do you know what yours says about you? Here's how to find out, and what to do if you find an inaccuracy.

Get Familiar with IDTF Supervision Requirements 9

Supervising tests at an IDTF can be tricky—here's what you need to know if your practice has an IDTF or a contract to supervise tests at one.

IN FUTURE ISSUES

- Don't Discuss Compliance Snafus Online
- Get Radiologists to Dictate Thorough Reports
- Be Prepared as FDA Targets Mammography Facilities

This newsletter has prior approval by the American Academy of Professional Coders for up to 10 CEUs per year. Granting this approval in no way constitutes endorsement by AAPC of the program, content, or the program sponsor.

Go to www.aapcnatl.org or call the AAPC at 1-800-626-2633 for more information.



Take Nine Security Measures When Employee Quits or Is Fired

Firing an employee is hard enough. But if you fail to promptly eliminate the employee's access to health information, you may be creating another problem—a serious security risk. This could also be true when an employee quits.

The proposed HIPAA security regulations address this risk by requiring that you adopt termination procedures that apply whenever an employee quits, is fired, or changes job responsibilities within the practice. The proposed regulations set four security measures that you must include in your termination procedures. We'll tell you about these measures, as well as five additional security measures that data security officer Chris Apgar recommends you also include when creating or updating your practice's employee termination procedures.

And we've given you a Model Checklist on p. 3 that you can adapt. You can use it to help you take the appropriate security measures whenever an employee quits, is fired, or changes job responsibilities.

1) Remove Employee's Access Privileges/User Accounts

Cutting off the employee's access to data is the third requirement in the proposed security regulations, but Apgar recommends that it be the first security measure you consider whenever an employee quits or is fired. If you fire the employee, it's critical to remove the employee's access rights to the information, services, and resources available on your practice's information systems as soon as possible. When an employee quits, you'll want the employee's access ended as soon as he or she leaves, and possibly much sooner, depending on the circumstances.

In most cases, deleting system-wide access rights can be done quickly and efficiently. Typically, you can delete or disable the employee's login ID and block the employee's access to the entire network. This is a fundamental security measure because, once it has been done, the likelihood of unauthorized access by the employee is nearly eliminated, Apgar says.

Insider Says: This and some of the other security measures (#2, #3, #4, #7, and #8) may also apply when an employee changes jobs within your practice because he or she may no longer need access to the same information. Previous access rights should be eliminated, and new access rights should be added as needed.

2) Remove Employee from Access Lists

Remove the employee from the access list of each program, system, and subsystem within your practice. This step protects systems and applications that may not be covered by the main network, such as remote-access programs, human resources, and accounting.

(continued on p. 2)

BOARD OF ADVISORS

- Andrei Costantino**
Parente Randolph Orlando
Carey & Associates, LLC
Harrisburg, PA
- William G. Franz Jr.**
Radiologix, Inc.
Dallas, TX
- Alice G. Gosfield, Esq.**
Alice G. Gosfield &
Assocs., PC
Philadelphia, PA
- Thomas W. Greeson, Esq.**
Reed Smith LLP
Falls Church, VA
- Karol Handrahan**
University of Maryland
Dept. of Radiology
Baltimore, MD
- Matthew Kupferberg, Esq.**
Harris Beach LLP
New York, NY
- Roberta J. Miller**
Medical College of Ohio
Dept. of Radiology
Toledo, OH
- Ronald E. Miller**
Medical College of
Virginia Hospitals
Richmond, VA
- Diane S. Millman, Esq.**
Powers Pyles Sutter
& Verville
Washington, DC
- Melody Mulaik, MSHS, CPC**
Coding Strategies, Inc.
Dallas, GA
- Claudia A. Murray**
Provider Practice
Analysis, LLC
Baldwin, MD
- Paula Richburg**
QuadraMed
Columbia, MO
- William A. Sarraille, Esq.**
Arent Fox Kintner Plotkin
& Kahn, PLLC
Washington, DC
- Michael F. Schaff, Esq.**
Wilentz Goldman & Spitzer
Woodbridge, NJ
- Jay Silverman, Esq.**
Ruskin Moscou Evans &
Faltischek PC
Uniondale, NY
- John R. Steiner, Esq.**
The Cleveland Clinic
Foundation
Cleveland, OH
- Tobin N. Watt, Esq.**
Smith Helms Murliss &
Moore, LLP
Atlanta, GA

Editor: **Jill K. Gormley, Esq.**

Executive Editors: **David B. Klein, Esq.,
Nicole R. Lefton, Esq., Janet Ray**

Senior Legal Editor: **Susan R. Lipp, Esq.**
Senior Editors: **Nancy Asquith, Heather Ogilvie**
Copy Chief: **Tamar M. Friedman**
Copy Editors: **Cynthia Gately, Graeme McLean**
Proofreader: **Lorna Drake**

Production Director: **Mary V. Lopez**
Senior Production Associate: **Sidney Short**
Production Associate: **Dennis T. Borruso**

Director of Planning: **Glenn S. Demby, Esq.**
New Projects Editor: **Rebecca L. Margulies, Esq.**

Director of New Media: **Michael T. Borruso, Esq.**

Marketing Director: **Peter Stowe**
Direct Marketing Manager: **Thomas A. Giordano**
List Management Director: **Vijay Thakkar**
Data Processing Manager: **Rochelle Conti**

Director of Operations: **Michael Koplin**
Sales Manager: **Joyce Lembo**
Customer Service Rep.: **Helena Thereso**
Fulfillment Supervisor: **Edgar A. Pinzón**

Financial Manager: **Janet Urbina**

Publisher: **George H. Schaeffer, Esq.**

Founders: **Andrew O. Shapiro, Esq.,
John M. Striker, Esq.**

Subscriptions: *Radiology Administrator's Compliance & Reimbursement Insider* (ISSN 1527-2338) is published monthly. Subscription rate: \$355 for 12 monthly issues. Address all correspondence to: Brownstone Publishers, Inc., 149 Fifth Ave., New York, NY 10010-6801. Tel.: 1-800-643-8095 or (212) 473-8200; fax: (212) 473-8786; e-mail: jgormley@brownstone.com

Disclaimer: This publication provides general coverage of its subject area. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional advice or services. If legal advice or other expert assistance is required, the services of a competent professional should be sought. The publisher shall not be responsible for any damages resulting from any error, inaccuracy, or omission contained in this publication.

© 2002 by Brownstone Publishers, Inc. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without written permission from the publisher.

TAKE NINE SECURITY MEASURES (continued from p. 1)

This is a straightforward task that can be completed relatively quickly. You simply remove the employee's name from each access list. If this precaution isn't taken, warns Apgar, there's a risk that a disgruntled ex-employee could get into the main system from a remote location and gain access to the practice's information systems.

3) Change Locks

Changing locks is a simple but valuable way to protect buildings, offices, property, equipment, and storage areas from unauthorized use and access. You may have to change door locks, alphanumeric punch codes, combination locks, and any other locks that provide employees with physical access. And if your employees use individualized access cards, you can—and should—disable the card from the system, Apgar points out.

The proposed security regulations require that you adopt a procedure for changing locks whenever an employee quits, is fired, or his or her access privileges are changed. They also require you to have a procedure for changing locks on a regular basis—say, every six months—to reduce the likelihood of unauthorized access by outside intruders. But keep in mind that the proposed security regulations are flexible and allow you to adopt a procedure that makes sense for your practice.

For example, many office buildings use numerical access codes to control entry. But because so many people use those codes, it would be impractical to adopt a procedure that requires changing the access codes each time an employee who works in the building quits or is fired. In that case, it may make sense for the practice to focus on protecting other areas of employee access.

4) Get Back All Keys, Access Tokens, and Other Access Devices from Employee

Whether or not you'll change the locks, you should get the employee to return all of the physical items that allow access to your practice. This includes keys, tokens, individualized access cards, and parking garage cards. If you can retrieve these items when—or even before—the employee leaves, you'll reduce the risk that the employee will copy them, give them to someone else, or never return them. Once an employee is gone, it's much tougher to retrieve these items.

Insider Says: It's also a good idea to require the employee to immediately return all other property belonging to your organization, suggests Apgar. For example, some practices provide employees with laptop computers. And telecommuters have the use of home computers, fax machines, software, beepers, cellular phones, and other equipment. These items are used to perform job functions from remote locations and store confidential or proprietary information. Your termination procedures should state that these items and the information maintained on them are the property of the employer and must be returned to the employer when employment ends.

5) Fire Employee or Discuss Voluntary Departure in Private

Firing an employee can be uncomfortable for all parties, including the employee's coworkers. So give the employee the bad news in private and in a profes-

sional manner. The same is true when an employee quits. If the employee begins the conversation in a public area, try to move it to a private setting.

This simple practice will help avoid a public scene, especially if an employee becomes visibly angry or harbors ill will toward you. It will also help you avoid the risk that an angry employee may disclose confidential information during a public scene. And talking privately with the employee can help to minimize workplace rumors that start when someone is fired in a common area.

6) Document Reasons for Firing Employee

Before you fire an employee, make sure the employee's personnel file includes the appropriate documentation supporting the reasons for termination, recommends Apgar. This practice makes good sense for several reasons. First, the proposed security regulations require this documentation if the employee is fired for a security violation. Second, gathering documentation after the fact may be hard if, for example, the paperwork is located in different departments. Third, if the documentation is created after termination, it's more likely that some facts will be unclear or forgotten. And fourth, there's always a risk that the employee will sue you for wrongful termination or a related claim. But having all the paperwork in order ahead of time will help you defend against such claims.

7) Remind Employee of the Duty to Maintain Confidentiality

Take the opportunity to remind the employee that he or she is legally and ethically obligated to maintain the confidentiality of patient and other sensitive information even after the

employee leaves your practice. If the employee signed a confidentiality agreement upon employment, give him or her a copy of it, if feasible, and document that fact in the employee's personnel file.

8) Conduct an Exit Interview

If possible, conduct an exit interview with each employee who quits, is fired, or transfers to another department, suggests Apgar. It's always important to get feedback from your employees. And employees who are

leaving can be a great source of information because they may discuss their likes and dislikes more openly.

Create a list of questions to ask the employee during the exit interview, and document the responses. Subjects to ask about include reasons for leaving (if voluntary), the work environment, employee morale, problems the employee has encountered, and suggestions for improvement. Also ask specific

(continued on p. 4)

MODEL CHECKLIST

Track Security Measures Taken When Employee Leaves

Here's a nine-point checklist of measures to take to protect the security of your organization's information when an employee is fired, quits, or changes positions within the organization. You can adapt the security checklist to use yourself and/or distribute it to your supervisory staff for quick reference. The first four security measures on the

checklist are included in the HIPAA proposed security regulations. Security measures #5 through #9 were provided by data security officer Chris Apgar. Some of these measures won't apply in every circumstance.

Show this checklist to your attorney. He or she may have other suggestions that are appropriate for your practice.

EMPLOYEE TERMINATION PROCEDURE CHECKLIST

Whenever an employee quits, is fired, or changes job responsibilities, initial and date each applicable item of this checklist as it's completed.

- Immediately remove employee's system-wide access privileges/user accounts.
- Immediately remove employee's name from access lists.
- Immediately change locks that employee had access to: buildings, offices, property, equipment, and storage areas.
- Collect all keys, tokens, access cards, and other access devices from employee before he/she leaves.
- If employee is being fired, notify him/her in private (if employee quits, try to move the conversation to a private setting).
- Document the reasons for termination in employee's personnel file.
- Remind employee of his/her legal and ethical duties to maintain the confidentiality of patient and sensitive information disclosed during the term of employment, and provide a copy of any confidentiality agreement the employee signed.
- Conduct an exit interview with employee as soon as possible, and document it.
- Provide last paycheck, return employee's personal belongings, and escort employee from the building if necessary.

TAKE NINE SECURITY MEASURES

(continued from p. 3)

questions about security issues (for example, is the employee aware of any security violations, was security training and education adequate, and were the penalties for security violations fully explained?). Responses to these questions will help you meet the proposed HIPAA requirements of assessing security risks, documenting security incidents, and keeping your security policies current, Apgar says. Also, remind the employee of his or her duty to maintain confidentiality, and give him or

her a copy of any confidentiality agreement if you were unable to do that before, says Apgar.

9) Give Employee Last Check and Belongings, and Escort from Building if Necessary

If the employee is being fired, be prepared to give the employee his or her last paycheck and personal belongings, and an escort from the premises if necessary. Although this step isn't necessary for every employee or every situation, it's good practice when you're dealing with an employee

who's angry or violent, has high-level access rights, or poses a major security threat. In certain circumstances you may want to take a similar approach with an employee who's quitting.

Once the employee has his or her paycheck and property, you've removed any legitimate reason for the employee to return to the premises, says Apgar. ■

Insider Source

Chris Apgar: Data Security Officer, Providence Health Plan, 3601 SW Murray Blvd., Ste. 10, Beaverton, OR 97005.

How to Avoid Trouble as Insurers Target 'Over-Reads'

It happens all the time—a practice's senior radiologists are on an insurer's panel, but the practice's junior radiologists aren't. In such cases, the insurer will pay only for interpretations performed by the radiologists on the panel. In a busy practice, it's often difficult to separate the patients by insurer. Ideally, a practice wants to be sure that only a radiologist who's on the insurer's panel does the interpretations for patients covered by that insurer. But many practices let any available radiologist do the initial interpretation, and then have a radiologist who's on the insurer's panel do an "over-read" later so that the insurer will reimburse the practice for the interpretation.

Although this is an increasingly common practice, it's a dangerous one, says New York health care attorney Jay Silverman. Insurers are using aggressive enforcement measures to cut their costs in these economically slow times, and that means they're coming down hard on practices they think are engaging in fraudulent over-reads. Silverman

reports that his firm is currently defending several radiology practices against insurers' allegations that the practices were billing fraudulently for over-reads.

We'll explain why these over-read arrangements are a problem and tell you the consequences if your practice is caught. And we'll give you some suggestions on how to prevent this problem in the first place.

Over-Reads Purely for Reimbursement Are Fraudulent

Sometimes practices don't see anything wrong with doing over-reads for reimbursement purposes since the initial interpretation is done by a radiologist. But insurers don't see it that way, Silverman says. They think it's fraud if an over-read is done just so that a practice can be reimbursed for an interpretation—and they're right.

Under Medicare rules—and the rules of nearly every health insurer—an over-read is reimbursable only if

the initial interpretation is equivocal, or if the interpreting radiologist requests a colleague's assistance in making a diagnosis. "If there's no medical reason for doing an over-read, then there's no legal way to submit a claim for reimbursement for the over-read," Silverman warns.

Getting Caught Equals Big Trouble

Some practices get careless because they think that if they get caught, they'll just have to pay back the insurer for any over-reads it disallows, Silverman remarks. But the consequences of getting in trouble with an insurer over billing improperly for over-reads can be far-reaching and devastating to a practice, he cautions.

Insurer may want its money back for every over-read. If you're very lucky, the insurer may request only that you repay it for the over-reads that were done for reimbursement purposes, plus the insurer's costs or an administrative penalty. More likely, though, the insurer will demand that you repay it for *every*

over-read for which it reimbursed your practice—even though many of those over-reads may have been medically necessary. The insurer will shift the burden onto you to demonstrate the medical necessity of every over-read you think is legitimately reimbursable. That can be a huge undertaking.

Insurer may kick you off its panel. Insurer contracts generally permit the insurer to terminate a physician or practice from the panel immediately with cause—and fraudulent billing is definitely cause. If the insurer kicks your practice off its panel, you'll not only lose patients—the insurer is also likely to share this information with other insurers. So shortly after one insurer terminates your practice, you may find that other insurers you contract with will send you letters asking for money back. And these other insurers may kick your practice off their panels, too.

Insurer may report you to the Integrity Databank. Most physicians are familiar with the National Practitioner Databank. But now there's an additional government databank, the Health Care Integrity and Protection Databank, which keeps track of problems physicians have had with third-party payors—including insurers. If an insurer can prove that you've billed it improperly, it may report you to this databank. And that can lead to a host of other problems, including inquiries from Medicare and Medicaid, as well as from other insurers you contract with, and even from your hospital and state licensing board, Silverman says.

Insurer may report you to your state licensing board. Some insurers may not bother to investigate your practice, but instead will report

their suspicions directly to your state licensing board. This can be a disaster, says Silverman, because state licensing boards are notorious for coming down hard on physicians whom they suspect of lacking integrity. And the process can be unfair because many states accept anonymous reports of physician wrongdoing. Even if the insurer doesn't make the report anonymously, almost every state protects the identity of the source of negative reports, Silverman says. In practical terms, that means the odds are stacked against you because you won't know who reported the alleged wrongdoing.

Insider Says: For more information about dealing with state licensing boards, see "How to Handle State Medical Licensing Board Inquiries," August 2001 *Insider*, p. 1.

Take Three Precautions to Avoid Over-Read Problems

The consequences of billing inappropriately for over-reads are just not worth the risk, Silverman says. He suggests taking three steps to avoid having to deal with this situation:

1) Try to negotiate your insurer contracts to include on their panels all the practice's radiologists. You could avoid the temptation to bill for unnecessary over-reads if you get all the radiologists in your practice on the insurers' panels. Too many practices feel that they have no negotiating power with insurers, so they don't even try to negotiate, Silverman says. But he has had some success getting managed care plans to accept on their panels all licensed physicians in a practice. So, he says, other practices could have similar success.

Insider Says: For more information on negotiating with insurers, see "Get Plans to Pay for Services From

Uncredentialed Providers," February 2001 *Insider*, p. 7, and "Plugging Loopholes: Make Sure New Employees, Partners Are Included in Your Plan Contracts," July 2000 *Insider*, p. 7.

2) Document medically necessary over-reads thoroughly. Sometimes a radiologist who does the initial interpretation wants or needs input from another radiologist to make a definitive diagnosis. In a case like this, it's absolutely appropriate to bill for an over-read, Silverman says. But thorough documentation is key. In his report, the radiologist who does the initial interpretation should be very clear about what aspect of the interpretation or diagnosis gave him trouble. And the radiologist who does the over-read should be equally explicit and detailed in her interpretation, Silverman emphasizes. It's important to realize that over-reads are more likely to be audited than are straight interpretations. So the documentation must be thorough and clear enough to show the auditor immediately that the over-read was appropriate and medically necessary, he explains.

3) Recognize that you may have to absorb some costs in the interest of patient care. If you can't get your newer radiologists on your insurer panels, then you're going to have to bite the bullet once in a while and absorb the costs of interpretations they do, Silverman says. For example, there will likely be times when a patient needs to have an interpretation, and the radiologists on the insurer's panel aren't available. In those cases, your first priority must be patient care, Silverman says. ■

Insider Source

Jay Silverman, Esq.: Ruskin Moscou Evans & Faltischek, PC, East Tower, 15th Fl., 190 EAB Plz., Uniondale, NY 11556.

ASK THE INSIDER

RACRI welcomes questions from subscribers. You can 1) send your questions to Brownstone Publishers, Inc., "Ask the Insider," 149 Fifth Ave., 16th Fl., New York, NY 10010; 2) fax them to (718) 243-2298; 3) call (718) 243-2337, and speak with the editor; or 4) e-mail them to jgormley@brownstone.com

Hospital-Based Practice May Bill Globally in Certain Circumstances

Q We're a radiology practice based at a small community hospital. We own our equipment and have a contract to provide radiology services to the hospital's patients. It would be convenient for us to bill globally, but I believe hospital-based departments can't do that. May we bill Medicare directly for both the professional and the technical components of our services?

A Maybe, says radiology coding consultant Melody Mulaik. Typically, the hospital owns the radiology equipment and bills Medicare or a third-party payor—or the patient—globally for radiology services (paying the radiologists a salary for their professional services). But it's possible for your hospital-based practice to bill Medicare and other payors globally for the technical and professional services you provide, if you meet the following requirements:

- The practice must own the equipment it uses in the performance of its professional services, or rent it for fair market value;

- The practice must directly employ the staff necessary to perform radiology services, including techs and clerical support staff;

- The practice must either perform its own coding and billing or reimburse the hospital for the fair market value of any coding and billing services the hospital performs on the practice's behalf;

- The practice must pay the hospital a fair market value rent for any space the practice occupies that the hospital owns; and

- Any payment from the hospital to the practice (for weekend and evening on-call services, for example) must be consistent with the fair market value of the services the practice provides.

These arrangements can be complicated to set up correctly, so be sure to get help from an experienced health care attorney, Mulaik recommends.

Insider Source

Melody Mulaik, MSHS, CPC: President, Coding Strategies Inc., 168 N. Johnson St., Ste. 103, Dallas, GA 30132.

Billing for Mammogram of Patient with Breast Implants in Absence of Signs or Symptoms

Q I noticed that in my new ICD-9 book, there's now a diagnosis code for breast implants—V50.1. Does this mean that CMS has changed its view on mammograms for patients with breast implants? Can we use this code to bill a diagnostic mammogram for a patient with breast implants but without signs or symptoms of breast disease?

A No, says Georgia-based radiology coding consultant Cindy Parman. Billing mammography for patients with implants has been a sticky issue for years, and the new diagnosis code isn't going to clarify it.

It's CMS's policy that a mammogram that's ordered in the absence of signs or symptoms of breast disease is a screening mammogram—period. Many radiologists believe that a mammogram for a patient with implants should be reimbursed at a higher rate because it requires at least three views of the breast, instead of the two standard views that a

mammogram for a patient without implants requires. But CMS doesn't see it that way, and its policy is to reimburse the same amount regardless of how many views of the breast are required.

You can use the V50.1 code as a diagnosis code for patients with cosmetic breast implants—but don't assume that a patient with implants got them for purely cosmetic reasons, Parman emphasizes. Sometimes breast augmentation is medically indicated. Make sure your office gets a thorough history of the patient that would indicate if there was any medical reason for the augmentation. And make sure your coders make their coding choices based on the documentation in the patient's chart, including that history, she says. ■

Insider Source

Cindy Parman, CPCH: Coding Strategies, Inc., 168 N. Johnston St., Ste. 103, Dallas, GA 30132.

Protect Yourself from Inaccurate Data Bank Reports

You're probably familiar with the National Practitioner Data Bank (NPDB). It's a repository of information about physicians reported by a variety of sources, including medical malpractice insurers, state medical licensing boards, hospitals, and professional societies. There's a second data bank, too, called the Health Care Integrity and Protection Data Bank (HIPDB), that contains information about criminal prosecutions related to health care and nonmalpractice lawsuits against health care providers. Hospitals must check these data banks whenever a physician applies for clinical privileges and every two years thereafter. Insurers check the data banks when deciding whether to include a physician on their provider panels. And when a practice is thinking of hiring a physician, it will often ask the physician to provide recent copies of his data bank reports, which show basic information, such as degrees and licenses, as well as the information reported to the data banks.

Even though most physicians know that the data banks exist and what sensitive information they contain, most of them don't regularly check to see if they're listed in the data banks or what the data banks' reports say about them. This is a mistake, says New York health care attorney Matthew Kupferberg. The NPDB has had problems with the accuracy of its information. Also, its efficiency in correcting errors has been questioned. In fact, the United States General Accounting Office (GAO), which is the office that investigates the efficiency of government programs, released a report in November 2000 called "Major Improvements Are Needed to Enhance Data Bank's Reliability."

It's your responsibility to make sure the data banks don't have inaccurate information on file about you, Kupferberg says. To do this, you'll have to check the data banks periodically. We'll tell you how to do this. Plus we'll give you the rundown on how to correct information in your reports that you think is inaccurate. And we'll tell you how to write an explanation of accurate—but negative—information about you so that you can tell your side of the story. Finally, we'll show you how to request an official review of information that you think is inaccurate.

How Can Inaccuracies Occur?

The NPDB gets information from "reporting entities" about "reportable events," says Kupferberg. Reporting entities include hospitals, licensing boards, insurance plans, professional liability insurers, and professional societies. "Reportable events" include malpractice verdicts or settlements, limitations or restrictions on hospital privileges, final actions against a medical license, and dismissal from a professional society for reasons relating to unprofessional or unethical conduct.

Health care plans and government agencies must report information about providers to the HIPDB. They must report any criminal and nonmalpractice civil judgments against providers for reasons related to health care, licensing and credentialing actions against providers, and Medicare and Medicaid exclusion actions.

Sometimes the information reported to a data bank isn't accurate. According to the GAO report, that's usually because the information was incomplete or just wrong.

Incomplete information. Missing information can do a lot of damage. For example, suppose that last year you were slapped with a lawsuit for a missed diagnosis. Your services met the appropriate standard of care, but your insurance company decided to settle because the plaintiff was a sympathetic person who had had a very bad treatment outcome. That settlement will be reported to the NPDB, and there's nothing you can do about it. But NPDB rules require an insurer reporting a malpractice payment on behalf of an insured physician to say whether the insurer considered the physician's standard of care when deciding to either settle or go to court, Kupferberg explains. This helps distinguish the "nuisance suits" from the egregious lapses in medical judgment. If the insurance company's information is incomplete—that is, it doesn't say that your standard of care was appropriate—your NPDB report will look worse than it should. The GAO says that information on malpractice settlements often doesn't indicate whether the physician met the appropriate standard of care.

Erroneous information. Sometimes reporting entities make inadvertent mistakes when they report information to the data banks. The GAO gives this example of a common error: A hospital may report restricting a physician's clinical privileges but mistakenly use a code in its report that indicates the physician's license has been revoked. An error like that creates enormous difficulty if it's not detected and fixed immediately.

Check Your Reports Every Year

Your data bank reports will list your name, state where you're licensed,

(continued on p. 8)

INACCURATE DATA BANK REPORTS

(continued from p. 7)

and other credentials. You should verify that this information is correct. And if a reporting entity has reported information about you—say, about a malpractice case or a problem with your hospital—you need to carefully review it for accuracy. The data banks are supposed to mail a notice and a copy of the information to you as soon as it's been submitted. But just because you haven't gotten a notice from one of the data banks doesn't mean no one has reported information on you. Maybe you've moved recently, and the notice went to the wrong address. Maybe it got lost in the mail. Or maybe, because of some glitch, it was never sent.

To be sure you know what the data banks say about you, request a copy of your reports at least once a year, Kupferberg suggests. It's easy to do and costs only \$20. Just go to the databank Web site at www.npdb.com, and click on "Report to and Query the Data Bank." Then click on "Self-Query Forms," and pull up the form for individuals. Fill out the form, print it out, have it notarized, and send it in to the address listed on the form. You need to fill out only one form to get a copy of the reports from both data banks. Your reports will arrive a week to 10 days later.

Correct Inaccuracies

If you discover that the data banks have gotten inaccurate information about you, there are several things you should do:

File a dispute form. The first thing to do is officially dispute the inaccurate information. When you get your data bank reports, you'll also get a form you can use to start a dispute. Once you file a properly

completed dispute form, the data bank will put a note in your report indicating that you're disputing it. That way everyone who checks the data bank until the dispute is settled will know about your objections.

Check with your attorney before completing the dispute form. It's trickier than you think. For example, you can use the dispute process only to:

- Supplement an incomplete report;
- Challenge the factual accuracy of a report; or
- Argue that information should be deleted because it deals with a "non-reportable event"—a hospital action that doesn't involve limiting your privileges, for example.

But you can't use the dispute process to question an insurer's decision to settle a case. And you can't use it to claim that a hospital's or licensing agency's action against you wasn't justified. If you file a dispute form that deals with anything other than disputing the completeness, factual accuracy, or the legal appropriateness of a report, the data bank will return the dispute form to you and won't note the dispute in the report on you, Kupferberg says.

Contact reporting entity. After you've filed a properly completed dispute form, you must also contact the reporting entity that supplied the information and ask it to change or void it, Kupferberg advises. Most reporting entities are willing to do this when it's appropriate. A polite letter pointing out the error or deficiency, with a copy to your attorney, is often all it takes, he says.

The notation that you've disputed the report will remain in your data bank report until the reporting entity notifies the data bank that it wants to:

- Correct the report;

- Void the report; or
- Decline to change the report.

Tell Your Side of the Story

Maybe the dispute process didn't result in a change to the report that satisfies you. Or maybe a report is accurate and complete, yet there are mitigating or extenuating circumstances that you would like people checking the data bank to know about. If so, you can submit a 2,000-character statement explaining the circumstances. Both data banks allow you to do this. Anyone who gets your data bank report will get the statement, too.

Kupferberg cautions that you should think carefully about what you have to gain by submitting a statement. Sometimes a physician suffering from wounded pride reacts emotionally to the report, and his statement does more harm than good. For example, if you submit a statement denying an objective third party's findings or claiming that the process was biased or unfair, it's not likely to help you. But suppose your hospital's peer review committee limited your privileges because it thought you needed additional training, and you got it—and the committee's decision wasn't based on a bad patient outcome. Then it's probably worthwhile to submit a statement saying that you were willing to get additional training to improve your skills, and no patient harm occurred, Kupferberg says.

If you decide to submit a statement, here are a few pointers:

- Try to avoid blaming others or denying responsibility for the problem;
- Stick to a dry recitation of the facts, emphasizing those facts that reflect positively on you;
- Get your attorney or an objective person you trust to help you write

the statement, or at least to read it before you submit it; and

- Be brief—2,000 characters means a total of 2,000 letters, spaces, and punctuation marks—not words. Use the character count function on your computer to be sure you don't go over the limit because the data bank will end the statement at 2,000 characters, even if that's in the middle of a word.

Ask for Secretarial Review as a Last Resort

If the reporting entity refuses to change or void the information it has reported, which you believe is inaccurate, there's a formal mechanism you can use to get a factually inaccurate data bank report changed. It's called a Secretarial Review. That is, the Secre-

tary of the Department of Health and Human Services will review the report and your objections to it. The process is time-consuming and can be expensive, Kupferberg notes, because you should get an attorney's help to request the review.

To request a Secretarial Review, complete a form that the data bank will send you when you first dispute the report. You must submit a written narrative with the form, which must:

- Describe which facts are in dispute;
- Give your version of the facts;
- Detail the efforts you've made to have the reporting entity change or void the report;
- Include documentation that supports your version of the facts; and

- Not exceed 10 pages—including your documentation.

Submit the form and narrative to the appropriate data bank, which will forward it to the office that conducts Secretarial Reviews, Kupferberg explains. It will probably be several months before you get a decision. If the Secretary concludes that the report is accurate or that the issues in dispute are outside the scope of Secretarial Review, the report will remain as is. But if the Secretary concludes that the report is inaccurate, the report will be removed from the data bank. ■

Insider Source

Matthew Kupferberg, Esq.: Harris Beach LLP, 500 Fifth Ave., 5th Fl., New York, NY 10110.

Get Familiar with IDTF Supervision Requirements

Medicare reimburses diagnostic tests performed at independent diagnostic and treatment facilities (IDTFs)—facilities not associated with hospitals—at a higher rate than it reimburses hospital outpatient clinics. As a result, many radiology practices are establishing IDTFs to help offset declining reimbursement for radiological services. Also, some radiologists and radiology practices are signing contracts with IDTFs to provide physician supervision of the tests the IDTFs perform.

But the physician supervision requirements at IDTFs can be tricky, says Virginia health care attorney Thomas W. Greeson. Many radiologists mistakenly assume that the same Medicare supervision rules that apply to diagnostic tests performed in their offices apply to tests performed in IDTFs. Although

all tests that require general or direct supervision in a physician's office will also require general supervision in an IDTF, additional requirements apply to those tests if they're performed in an IDTF, Greeson says. If your radiologists aren't familiar with the additional supervision requirements that apply to IDTFs, they could find themselves in hot water—whether they're the owners of the IDTF or the supervising physicians.

We'll tell you what special qualifications physicians need to supervise tests in an IDTF—not just any physician will do. And we'll describe the IDTF supervising physician's added responsibilities, which include monitoring the quality of the images, calibrating the equipment, and verifying the credentials of the technologists.

Special Qualifications Necessary to Provide Supervision at IDTFs

Under the Medicare supervision rules that most physicians are familiar with, each diagnostic test performed by nonphysician personnel requires either the physician's general, direct, or personal supervision. For a test performed in a physician's office, the supervision of any licensed physician will do. But according to Medicare supervision rules, the supervising physician at an IDTF must be able to provide evidence demonstrating her "proficiency in the performance and interpretation of each type of diagnostic procedure performed by the IDTF."

Greeson offers the following example: If the IDTF performs MRIs, then the carrier may ask every

(continued on p. 10)

IDTF SUPERVISION REQUIREMENTS

(continued from p. 9)

physician at the IDTF who supervises these tests to demonstrate proficiency in performing and interpreting MR images—even if the supervising physician won't actually be taking or interpreting the images. Just being a physician isn't enough in itself, so check with your carrier for its interpretation of "demonstrated proficiency."

Supervising Physician at IDTF Has Special Duties

Being a supervising physician at an IDTF entails a lot of responsibility, Greeson says. The supervising physician doesn't just need to be available in case of emergency, or to answer a technologist's question. Medicare's IDTF supervision rules require the supervising physician at an IDTF to take responsibility for many aspects of the IDTF's operation, Greeson explains. These include:

Oversight of test quality. A supervising physician at an IDTF must monitor the quality of the serv-

ices the IDTF performs, Greeson says. If Medicare becomes aware that an IDTF provides poor quality services, the supervising physician will be on the hook, Greeson cautions. And if a supervising physician should have discovered the quality deficiencies but didn't, or discovered these deficiencies but didn't take adequate action to improve the IDTF's services, the physician could be in big trouble.

What kind of trouble? Both Medicare and state licensing authorities could take action against the physician, says Greeson. Plus the physician could be named in a malpractice suit if the IDTF misdiagnosed a patient—even though the supervising physician never saw the patient and didn't provide the professional interpretation, Greeson notes.

Assure proper maintenance and calibration of equipment. Many supervising physicians at IDTFs don't realize that they're responsible for seeing that the IDTF's equipment is functioning properly, Greeson

asserts. So it's crucial that any physician who's supervising tests at an IDTF become an expert in the equipment that the IDTF uses. This may require some extra effort—but again, failure to uphold this responsibility could lead to problems with Medicare and the physician's state licensing board, as well as professional liability exposure.

Verification of techs' credentials. Medicare rules make the supervising physician at an IDTF responsible for ensuring that the non-physician staff members who perform the diagnostic tests are qualified to do so. At a minimum, the supervising physician must become familiar with the licensing requirements for the various technologists who will perform tests at the IDTF, and must review documentation proving that the employees have the necessary, specialty-specific qualifications, Greeson says. ■

Insider Source

Thomas W. Greeson, Esq.: Reed Smith LLP, 3110 Fairview Park Dr., Ste. 1400, Falls Church, VA 22042.