AMERICAN HEALTH CONSULTANTS

# COMPLIANCE HOTLINE™

THE NATION'S ESSENTIAL ALERT FOR HEALTH CARE COMPLIANCE OFFICERS

MONDAY
APRIL 1, 2002


## HHS proposes big changes to HIPAA privacy regulations

*But the changes to patient privacy regulations are likely to cut both ways, experts say*

The Department of Health and Human Services (HHS) has proposed major changes to the privacy regulations set to go into effect April 2003. Health care attorneys say the changes go further in relaxing some of the most onerous provisions than most observers expected. But like most things involving the Health Insurance Portability and Accountability Act (HIPAA), some changes fly in the opposite direction, they add.

Many of the changes contained in the proposed rule address problems identified by HHS in the guidance it released last summer, says **Rebecca Williams**, a partner with Davis Wright in Seattle. But some of the proposed changes not foreshadowed in the guidance are likely to be good news for the health care industry, she adds.

The most significant change would be the elimination of the need for a written patient consent to allow providers to use protected health information for treatment, payment, and operations, says Williams. Providers argued that requirement would impede access to care and did not give patients any real control over their health information. HHS apparently agreed. The new rule simply would require providers to use good-faith efforts to obtain a written acknowledgement of the receipt of their notice of privacy practices.

*See **Privacy changes**, page 2*

## Research institutions face growing false claims threat

Most compliance officers and others charged with overseeing medical research are well aware of recent actions by federal agencies such as the Food and Drug Administration and the Office of Human Research Protections that police clinical research. However, many are less familiar with the looming threat of the False Claims Act, warns **Paul Kalb**, who heads up the health care practice of the Washington, DC-based law firm Sidley and Austin.

Not only are the penalties associated with the False Claims Act potentially huge, the incentives for whistle-blowers are enormous, he cautions.

Kalb points out that federal grant monies are

*See **Medical research**, page 3*

## Decision addresses unclear fraud regulations

Health care entities that face prosecution over regulatory and statutory mandates that often are unclear or ambiguous can take hope in a recent decision by the Eleventh Circuit Court of Appeals, says False Claims Act expert **John Boese**, of Fried Frank in Washington.

Two weeks ago, a panel of the Eleventh Circuit reversed the convictions of two former employees indicted for filing allegedly false Medicare cost reports. The court held that the regulations at issue were unclear and that the government failed to prove that the defendants knowingly relied on an unreasonable interpretation of those regulations, Boese reports.

The decision could have "a very broad effect" on civil and criminal fraud cases in health care, according to Boese. The convictions were highly publicized examples of cases in which the prosecution relied on "extremely complex regulations

*See **Unclear regulations**, page 3*

# Privacy changes

*Continued from page 1*

The proposal also would give payers and providers more latitude in sharing health information for payment and operations, Williams says. Under the current rule, a covered entity can use health information for its own operational purposes, but there was confusion about whether a covered entity could disclose the information to another provider to obtain payment or for quality assurance or credentialing purposes. The proposed changes would permit the sharing of information for these and other similar purposes, she says.

That's the good news. The bad news is that what many consider to be the most burdensome aspect of the current rule — the minimum-necessary rule — was left largely unchanged, says **Paul Smith**, a Davis Wright partner in San Francisco. In this area, HHS merely repeats its earlier assurances that covered entities have flexibility to address their unique circumstances and can make their own assessment of what protected health information is reasonably necessary for particular purposes.

The proposed rule would explicitly permit incidental disclosures resulting from such activities as discussions at nursing stations, the use of sign-in sheets, and calling out names in waiting rooms, he adds.

According to **Leigh-Ann Patterson**, a partner with Nixon Peabody in Boston, the proposed regulation also would tighten the restrictions on health-related marketing activities. The current rule allows private health care information to be used for marketing purposes without prior patient authorization, as long as the solicitation or promotional materials contain certain disclosures and opt-out provisions.

Patterson says the proposed change closes this loophole by requiring prior patient authorization before any protected health care information may be used for marketing purposes. That means permission-based marketing programs no longer will be the exception, but rather the rule.

The proposed rule also would give covered entities an extension of up to one year to modify their business associate agreements, says **Steve Zubiago**, a Nixon Peabody partner in Providence, RI. Although HHS was urged to eliminate the business-associate contract requirement — which requires providers to secure contractual obligations from their business associates stating that they too will abide by HIPAA's privacy rule — HHS stood firm and instead attempted to make compliance less burdensome. Under the proposed change, covered entities will have until April 14, 2002, to amend their various contracts to incorporate the HIPAA privacy promise.

HHS is accepting comments on the proposed changes for 30 days. However, all sides expect the proposed changes to be fully implemented.

There still is considerable confusion regarding the manner in which privacy will be enforced by HHS. **Bill Braithwaite**, director at PriceWaterhouseCoopers in Washington, DC, says a good rule of thumb is this: "If you don't surprise the patient, you won't get into trouble." Sometimes, even if you do surprise patients, such as by publishing their e-mail address on the web accidentally, the damage can be ameliorated if they are contacted immediately, he adds.

According to Braithwaite, this approach is especially important in the area of medical research because many people in that environment are not accustomed to directly dealing with patients. "They forget that they are people rather than records in a database," he asserts. "They can cause you a lot of problems."

Braithwaite notes that providers now are waiting for the final rule for the HIPAA security requirements. The proposed rule for security was published in 1998, but the final rule has yet to appear.

*(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®.


**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 p.m. EST.

"It is kind of bizarre," asserts Braithwaite, who until recently was HHS' point man on privacy and security. "The final rule has been ready for many months," he says. "It was finalized as soon as the final privacy rule was finalized."

The rationale for delaying it until now was that privacy and security must operate together, says Braithwaite, noting that HHS now says it expects to publish the final security rule in the summer.

Regardless of when the final rule appears, Braithwaite says providers must know something about security. Not only has the proposed rule for security been published, but the final privacy rule includes several security concepts, he says.

"Knowing something about security even without the final security rule is important," he asserts. "The basic philosophy is expressed in the HIPAA law quite clearly — covered entities shall maintain reasonable and appropriate administrative, technical, and physical safeguards." ■

## Unclear regulations

*Continued from page 1*

whose interpretation was subject to legitimate dispute," he explains. "This decision may significantly limit such prosecutions in the future.

"This case provides an important affirmation that, in cases where the truth or falsity of a statement depends on a legal interpretation of a regulation, the government cannot simply show that its interpretation is preferable," he adds. "The government must prove the defendant's interpretation is unreasonably wrong."

According to Boese, many courts, particularly in the civil fraud area, have been willing to allow the government to proceed with fraud cases based on "clearly ambiguous regulations." He notes that two appellate courts have taken that approach in civil False Claims Act cases.

In one case, the Ninth Circuit reversed the dismissal of a *qui tam* False Claims Act case where the lower court held that the disputed claims could not be false because the defendants relied on a reasonable interpretation of an ambiguous regulation. The Eighth Circuit recently cited that case in another case involving ambiguous Medicare regulations *(Minnesota Association of Nurse Anesthetists v. Allina Health System).* ■

## Medical research

*Continued from page 1*

accompanied by the recipient's contractual obligations to use the money appropriately. When grant recipients accept reimbursement from the National Institutes of Health and other federal agencies, they do so with certification, he notes. "To the extent that monies have been used in ways that were not intended, those claims for reimbursement arguably are false and can give rise to liability under the False Claims Act," he warns.

The False Claims Act also can be used another way, says Kalb. Recipients of federal grant monies accept those funds subject to an agreement to abide by a dozen separate regulatory obligations, including regulations governing conflicts of interest and scientific misconduct. "If they seek reimbursement for the research without having fully complied with those regulatory obligations, then arguably the claims for reimbursement are false, he asserts.

Kalb says that several lawsuits in recent years have adopted the notion that noncompliance with a regulatory scheme that is a condition of reimbursement renders claims for reimbursement false. While those lawsuits have not involved enormous sums, he predicts they may become more common before too long.

**David Hoffman**, Assistant U.S. Attorney for the Eastern District of Pennsylvania, agrees that the key ingredient implicating the False Claims Act is the certification process. "When you are certifying to the government that certain things are happening, that is not just a rubber stamp," he asserts. "From the government's perspective, those certifications have meaning, and that is how you get to the application of the False Claims Act."

Hoffman says research institutions must establish systems to identify rogue employees internally before the government does. "That is especially the case now that Medicare is becoming more involved in paying for human subjects. The potential conflicts with researchers having an interest in licensing fees and royalties if things go well are very troublesome."

If you want to know where government enforcement agencies spend their time, you can simply

*(Continued on page 4)*

follow the money, says former Department of Justice attorney **John Bentivoglio**, now of Arnold and Porter in Washington, DC. "With the increasing amount of federal dollars going to biomedical research, if history is any guide, there will be an increasing amount of interest from the federal government in this area," he asserts.

Adding to that threat are issues that involve risk to patients, Bentivoglio says. Also high on the list are conflicts of interest and arrangements between industry and clinical investigators that might violate the anti-kickback statute. ■

# Five steps to successful research compliance

Government enforcement agencies have set their sights on research institutions. As a result, research compliance should be a vital component of any research institution's overall compliance plan, says **Sandy Piersol**, a senior manager with Deloitte and Touche in Philadelphia.

Piersol says the risk-assessment process for research institutions is the same as that used for other compliance programs. The principles can be fashioned into practical applications, and the same five-step risk assessment process can be applied within the research component of the institution regardless of whether it is for the whole institution, one clinical trial, or one department.

"The formula is simple," says Piersol. "Risk areas minus your controls equals your assessment of risk." She says a high risk accompanied by a lot of controls can become low risk. But without those controls, risk will remain high.

Piersol and **Kim St. Amant**, another senior manager with Deloitte and Touche in Boston, recommend these steps:

**I. Identify risk areas.** The first step is to identify risks and prioritize the high-risk areas, Piersol says. One important issue that research institutions should consider is what risk areas have special relevance to their research portfolio. Another is where the research enterprise may be vulnerable.

Risk areas are not static, risk assessment is not a one-time event, and on-going identification and monitoring of risk is mission-critical, warns St. Amant. Frequently, new laws and regulations as well as new interpretations must be considered. In addition, often there are new lines of business and new ways of doing things.

New staff often represent a risk area. "You may have done training last year and now have many people who are new to the organization," she says. "That can create risk in and of itself."

St. Amant says numerous sources can help identify risk areas, including documents from the Department of Human Services' Office of Inspector General, analysis of applicable laws as well as relevant lawsuits, *qui tam* cases, and settlement agreements.

**II. Prioritize high-risk areas.** It is important not to waste time on low-risk areas, warns Piersol. "You want to go right to the high-risk areas and prioritize those," she asserts. "It is essential to start with the risk areas that are likely to give rise to liability and dollars."

**III. Assess risk.** Piersol says research institutions also must determine the "current state" of compliance and ask themselves, 'Are we in compliance?' If an area is found not to be in compliance, organizations must learn why and then redesign internal controls, she says.

**IV. Analyze findings and solutions.** According to Piersol, research institutions must seek to understand the cause and extent of the problems identified. "Once you identify a problem, you must dig deeper to find out the root cause," she explains.

However, every rumor does not warrant an investigation, says Piersol. Some concerns can be addressed to the compliance committee or other internal identity without inordinate resources. "The key is to act on it," she asserts.

**V. Operationalize corrective actions.** Prioritizing corrective actions and assigning accountability often can be the hardest step, says Piersol. That makes it critical to get the right people on board and develop a timetable, she says.

Corrective actions can be accomplished with policies, procedures, training, and monitoring and auditing. These steps often need to be repeated and, to be successful, should be "built-in" vs. "added-on." Only when processes are built into the fabric of the organization will people understand why certain steps are being taken, she says. ■