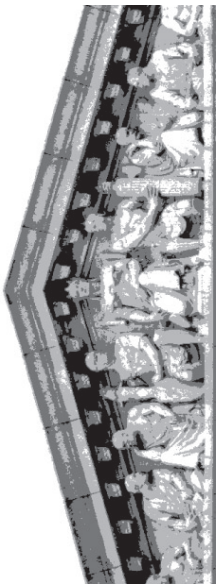


G-2 Compliance Report

WASHINGTON G-2 REPORTS

Vol. V, No. 6, June-July 2003

For Hospitals, Laboratories and Physician Practices

OIG Warns Drug Manufacturers About Suspect Business Practices

New compliance program guidance for pharmaceutical manufacturers sends a clear cautionary signal to drug companies that they can no longer conduct business as usual.

The final guidance, which appeared in the May 5 *Federal Register*, offers broad insight into what the HHS Office of Inspector General considers key risk areas in industry practices. As in the draft guidance released in October 2002, the OIG identifies three principal potential risk areas for pharmaceutical manufacturers:

1) Integrity of data used by state and federal governments to establish payment amounts
2) Kickbacks and other illegal remuneration
3) Compliance with laws regulating drug samples

While the final guidance contains no new legal obligations, it should be tapped by the drug industry as a starting point, the OIG says, for legal review of particular practices and development of policies to reduce potential risk. The document makes clear that the recommendations are not mandatory, but rather are a set of guidelines that pharmaceutical manufacturers should consider when developing and implementing a compliance program or evaluating an existing one.

Integrity Of Data

One area of the final guidance focuses on data submitted by pharmaceutical manufacturers in connection with government healthcare programs. The OIG is particularly concerned about determination of the Average Wholesale Price (AWP) under the Medicare

➥ *p. 2*

Inside this issue

OIG issues final guidance for pharmaceutical companies 2

CMS official named interim IG 3

Christus Health Affiliates reach settlement 3

ESRD lab payment under Medicare clarified 4

Six new CLIA waived tests cleared 4

Compliance officers face new challenges concerning patient safety: see *Perspectives* ... 5

HIPAA security standards matrix 10

Feds okay HCA settlement agreement 11

Providers on target to comply with HIPAA standards 11

For the Record: HIPAA & subpoenas 11

News in brief 12

Tips On Negotiating A HIPAA Security Contract

As healthcare providers begin preparing to implement provisions of the HIPAA final security rule, they should pay close attention to how they structure contracts with security consultants, advises attorney Dina Ross with McDermott, Will & Emery (Chicago, IL).

The final rule, mandated under requirements of the Health Insurance Portability & Accountability Act, takes effect Apr. 21, 2005, for most covered entities (small health plans have an additional year to comply). The rule, published in the Feb. 20 *Federal Register*, includes a security matrix that lays out standards and implementation specifications (*see chart, p. 10*) and helps clear up some of the confusion about how the standards align with the HIPAA final rule on medical privacy, which became effective on Apr. 14 of this year (*GCR, Mar. 03, p. 1*).

"The first decision you'll probably have to make as a covered entity is whether to do it yourself

➥ *p. 9*

Judith Waltz

Suspect Business Practices, *from p. 1*

program and rebates under the Medicaid Rebate Program, both of which depend on price and sales data that are either directly or indirectly furnished by pharmaceutical manufacturers.

The government expects that such data will be complete and accurate. While submission of false, fraudulent or misleading information may expose pharmaceutical manufacturers to liability under the federal False Claims Act and/or the anti-kickback statute, the guidance offers recommendations that may aid drug companies in avoiding liability. These include accurately taking into account price reductions, discounts for cash, rebates, goods in kind, free or reduced-price services and grants.

Kickbacks, Other Illegal Remuneration

The federal anti-kickback statute prohibits in the healthcare industry some practices that are common in other business sectors, notes the OIG. It advises manufacturers to identify any remunerative relationship with those in a position to generate federal healthcare business for the manufacturer directly or indirectly, and then determine whether any one purpose may be to induce referrals. A lawful purpose will not legitimize a payment that also has an unlawful purpose, says the guidance.

Though ultimate liability under the anti-kickback statute will hinge on the party's intent, the OIG suggests that identifying such arrangements will help manufacturers assess their risk. The guidance lists the following questions that drug manufacturers should ask about any problematic arrangement:

- Does it have a potential to interfere with clinical decision-making or undermine the clinical integrity of a formulary process? If it involves providing information, is the information complete, accurate and not misleading?
- Does the arrangement have the potential to increase costs to federal healthcare programs, beneficiaries or enrollees? Does it have the potential to be a disguised discount to circumvent the Medicaid Rebate Program Best Price calculation?
- Does the arrangement or practice have a potential to increase the risk of overuse or inappropriate use?
- Does the arrangement or practice raise patient safety or quality-of-care concerns?

In what appears to be recognition that not all "suspect" practices or activities are necessarily illegal, the guidance advises that the propriety of any particular arrangement must be based on a careful evaluation of the facts and circumstances. In some cases, an arrangement may be structured to fit into one of the safe harbors under the anti-kickback statute, says the OIG.

Drug Samples

Expressing concern about the improper sale of drug samples, the OIG recommends that pharmaceutical manufacturers closely follow the Prescription Drug Marketing Act of 1987 (PDMA), which governs the distribution of drug samples and forbids their sale. It appears that the OIG's concern stems from recent government investigations involving physicians who billed federal healthcare programs for drug samples they obtained at no cost.

Failure to comply with PDMA requirements can result in sanctions, the OIG warns, adding that improper use of samples may also trigger liability under the False Claims Act and the anti-kickback statute.

Don't Forget The Basics

While the final compliance program guidance focuses largely on anti-kickback issues, drug companies should also remain cognizant of more "garden variety" issues, such as violations of the False Claims Act, cautions Judith Waltz, a healthcare attorney with Foley & Lardner in San Francisco, CA.

"If someone is designing a compliance program based on this guidance, they need to remember the basics as well. I would advise drug companies to read the guidance and follow it, but not assume this is a complete package. This will give you a framework for your compliance program, but the risk areas should not be viewed as complete," she says.

Pharmaceutical manufacturers that already have an established compliance program should use the latest guidance to evaluate its effectiveness, Waltz notes.

Resources

- Judith Waltz: 415-438-6412
- OIG: Final Compliance Program Guidance For Pharmaceutical Manufacturers, *www.oig.hhs.gov/fraud/docs complianceguidance/042803pharmacymfgonfr.pdf*

Interim IG Named, Rumors About Permanent Replacement Abound

Dara Corrigan, director of program integrity at the Centers for Medicare & Medicaid Services, has been named acting principal deputy inspector general for the U.S. Department of Health & Human Services. In this position, Corrigan will function as interim IG, running the office until the Bush Administration nominates, and the Senate confirms, a successor to Janet Rehnquist, who resigned as IG effective June 1.

Corrigan takes over from Dennis Duquette, who was named to the acting post shortly after Rehnquist announced her resignation in March. Duquette is expected to return to his former role as deputy inspector general for audit services.

Meantime, speculation about who will be chosen as the permanent replacement for Rehnquist is rampant. Among those rumored to be in the running are David William, former IG of the Social Security Administration and the Internal Revenue Service, and former healthcare lawyer Harold Damelin, now the IG at the Small Business Administration. Justice Department IG Glenn Fine and Railroad Retirement Board IG Martin J. Dickman reportedly have already turned down the job.

Industry sources believe the White House is carefully scrutinizing potential replacements to ensure that the President's final choice is someone who can rebuild the credibility of the HHS OIG. Rehnquist resigned amid mounting discontent from Congress over allegations that she abused her powers (*GCR, Apr. 03, p. 1*).

Sen. Charles Grassley (R-IA), a vocal critic of Rehnquist, had planned to call for her resignation Mar. 10, but she formally relinquished the post in a letter dated Mar. 4. The General Accounting Office in late 2001 launched an investigation of her tenure as IG at the request of Grassley and other lawmakers. The GAO is expected to release a draft of its findings during the first part of June. The draft had been anticipated earlier in the spring. It goes first to the OIG for comment before being made public. The final version is now expected to be released by June 30.

Challenges Ahead

The new IG will face a number of challenges, attorney Kirk Nahra tells *G-2 Compliance Report*. Nahra, who is with Wiley Rein & Fielding (Washington, DC), says these include replacing senior management expertise that has been lost over the last two years, improving staffing levels and restoring a sense of mission and professionalism to the office.

"Presumably, the White House is looking for someone with a combination of skill sets and management experience," he says.

Convincing Congress to increase funding for fraud-fighting efforts will also be a challenge for the new IG, he adds. The OIG receives much of its funding through the Health Care Fraud & Abuse Control Program established under HIPAA (the Health Insurance Portability & Accountability Act of 1996). The funding ceiling has increased every year, but will level off in fiscal 2004. Congress would have to amend HIPAA to change the IG's mandatory funding levels.

"There's a pretty clear connection between funding, staffing and the amount of money the office recovers," Nahra points out. "Staffing is definitely pretty low right now. They've lost a lot of talented people."

Resource

❖ Kirk Nahra: 202-719-7335

Christus Health Affiliates Settle Fraud Charges

Three San Antonio affiliates of Christus Health of Houston have paid the Federal Government $1.36 million to settle allegations that they defrauded Medicare and Medicaid from 1997 through 2000, the U.S. Department of Justice announced May 7.

The civil settlement resolves allegations that Primary CareNet of Texas (PCN), a management and billing company (also known as Christus Primary CareNet), and two physician practice groups—Health Texas Medical Group (HTMG) on its own behalf and as successor in interest to Solomon Anthony Clinic (SAC)—improperly charged Medicare and Medicaid for physicians' evaluation and management services.

The allegations arose from a lawsuit filed by PCN's former chief financial officer, Timothy Ohman, under the *qui tam* (whistleblower) provisions of the federal False Claims Act.

CMS Clarifies Payment Policies For ESRD Lab Services

The Centers for Medicare & Medicaid Services is implementing new procedures to ensure that claims for laboratory services related to end-stage renal disease (ESRD) are properly submitted to Medicare.

In a May 2 program memo, the agency said it is making the changes in response to several studies by the HHS Office of Inspector General, which found that ESRD claims often are not paid in compliance with stated Medicare policy.

Medicare reimburses routine automated multichannel chemistry tests (AMCCs) for individual ESRD patients within the composite rate payment to ESRD facilities, according to the memo. Separate reimbursement can be made for clinical diagnostic laboratory tests performed on each service date when more than half of all tests are non-composite rate tests.

Other reimbursement conditions include:

- The lowest rate will be paid for services performed by the same provider for the same beneficiary on the same date.
- Intermediaries should identify by date of service which AMCC tests are included in the composite rate.
- When at least 50% of covered tests are included in the composite rate payment, all submitted tests are included in that payment, and no separate payment is made for any of the tests.
- When fewer than 50% of covered tests are composite rate tests, all AMCC tests can be reimbursed separately.

Three pricing modifiers identify the different payment situations for the AMCC tests. The physician ordering the test is responsible for identifying the appropriate modifier:

- CD: Tests that are part of the composite rate and not separately billable.
- CE: Tests that are composite rate tests but are beyond the normal frequency covered under the rate and are separately billable based on medical necessity.
- CF: Tests that are not part of the composite rate and are separately billable.

The transmittal also spells out information that intermediaries must post on their Website to educate providers about the billing procedures.

Resource

- Program Memorandum, Transmittal No. A-03-033: *http://cms.hhs.gov/manuals/memos/comm_date_dsc.asp*

FDA Grants CLIA Waiver To Six More Tests

The Food & Drug Administration has announced six new additions to the roster of tests it has cleared for waived status under CLIA (Clinical Laboratory Improvement Amendments of 1988). The tests and their CPT codes/HCPCS modifiers for billing Medicare are:

- 81003QW: Hypoguard Diascreen® Urine Chemistry Analyzer, effective Dec. 6, 2002.
- 83036QW: Bio-Rad Micromat II Hemoglobin A1c Prescription Home Use Test, effective Dec. 17, 2002.
- 86701QW: OraSure Technologies OraQuick Rapid HIV-1 Antibody Test, effective Jan. 31, 2003.
- 82273QW: Aerscher Hemaprompt FG, effective Feb. 11, 2003.
- 87880QW: Immunostics Immuno/Strep A Detector, effective Feb. 13, 2003.
- 87880QW: Stanbio QuStick Strep A, effective Mar. 5, 2003.

The waived category is the least regulated under CLIA, requiring only that CLIA-certified labs follow the manufacturer's instructions when using a waived test kit. The QW modifier indicates that the test, unless performed on a waived device, would otherwise be considered moderate or high complexity under CLIA.

Both 83036QW and 86701QW are subject to national coverage determinations. For more information, see Transmittal AB-03-056 at *http://cms.hhs.gov/manuals/memos/comm_date_dsc.asp*

COMPLIANCE PERSPECTIVES

Patient Safety, Medical Errors In The Compliance Spotlight

Dawn Kirschenman

Gay Fright

Dawn Kirschenman is a senior consulting manager and Gay Fright is an associate vice president with Misys Healthcare Consulting in Tucson, Arizona

"To err is human" is more than an old maxim—it's also the title of a major report, released in 1999 by the federal Institute of Medicine (IOM), which spawned much public concern over its assertion that medical errors were the 8th leading cause of death in the U.S.—with 44,000-98,000 deaths a year, at an estimated annual cost of $8 million.

The IOM advocated a comprehensive approach to improving patient safety with several recommendations, including:

- Create a Center for Patient Safety
- Create a nationwide mandatory reporting system
- Develop programs to encourage voluntary reporting systems
- Enact legislation to protect data that are collected and analyzed for purposes of improving safety and quality
- Set performance standards and expectations for healthcare organizations, with attention on patient safety
- Encourage health professional licensing bodies and professional societies to focus greater attention on patient safety
- Increase Food & Drug Administration attention on the safe use of drugs
- Encourage healthcare organizations to establish continuous safety improvement programs with executive sponsorship and highly visible goals

The IOM's second report, "Crossing the Quality Chasm: A New Health System for the 21st Century," encouraged "redesigned systems of care, including use of information technology to support clinical and administrative processes."

No doubt, these two reports from the IOM have driven a number of patient safety initiatives in healthcare. As a result, a myriad of legislative/governmental, regulatory and private-sector efforts have emerged to actively address patient safety issues. Their goals are similar, but each has a different focus. Healthcare providers and compliance officers are challenged to understand them and determine how these goals apply to their environment. The following are some of the most prominent organizations and their approaches to patient safety.

JCAHO

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) is a hospital-accrediting agency with established national patient safety goals to help accredited organizations address specific areas of concern. Each goal includes no more than two succinct, evidence- or expert-based recommendations.

Effective Jan. 1, 2003, all JCAHO-accredited healthcare organizations, or those seeking accreditation, will be surveyed (announced or unannounced) for implementation of six goals and 11 associated recommendations—or acceptable alternatives—as appropriate to the services they provide.

The six national patient safety goals are:

1) Improve the accuracy of patient identification
2) Improve the effectiveness of communication among caregivers
3) Improve the safety of using high-alert medications
4) Eliminate wrong-site, wrong-patient, wrong-procedure surgery
5) Improve the safety of using infusion pumps
6) Improve the effectiveness of clinical alarm systems

Since 1999, the JCAHO accreditation process has included organizations' sentinel-event activities. A sentinel event is defined as an unexpected occurrence involving death, serious physical or psychological injury or the

risk thereof. Serious injury specifically includes loss of a limb or function. The phrase, "or the risk thereof," includes any process variation for which a recurrence would carry a significant chance of a serious adverse outcome. Although sentinel-event reporting is voluntary, healthcare organizations are expected to complete a thorough, credible root-cause analysis, make improvements to reduce risk and monitor the effectiveness of those improvements for each sentinel event.

A benefit of sentinel-event reporting is that it helps track data for analysis and also provides information and education on safety problem areas to accredited organizations through JCAHO's Sentinel Event Alert periodic publication. The January 2003 edition emphasized a recommendation that healthcare organizations should manage, as sentinel events, all identified cases of death and major permanent loss of function attributed to a nosocomial infection.

Another JCAHO sentinel-event policy goal is to develop a Patient Safety Taxonomy. This would standardize patient safety terms and improve communication and data collection, classification, storage and analysis.

U.S. House Of Representatives

The House Ways & Means and Energy & Commerce Committees have approved similar medical error reduction bills—the Patient Safety & Quality Improvement Act (H.R. 663) and the Patient Safety Improvement Act of 2003 (H.R. 877). Both would establish a medical error reporting system. A counterpart to H.R. 663 has been recently introduced in the Senate (S. 720).

If enacted, the legislation would provide certification guidelines for creating Patient Safety Organizations (PSOs). Healthcare providers would voluntarily collect data for submission to a PSO, which would analyze the data and report back to providers on how to improve patient safety and minimize risk. The findings would be shared with other PSOs, and non-identifiable data would be submitted to a Center for Quality Improvement & Patient Safety for inclusion in a Patient Safety Database. This national medical error database would be used to analyze national and regional statistics, trends and patterns.

The bills establish privacy protections and employment protection for those who report the data. Another component creates a Medical Information Technology Advisory Board (MITAB), which would voluntarily develop and update national standards that promote the interoperability of information technology systems across all healthcare settings.

H.R. 663 would authorize grants to practitioners to establish electronic prescription programs, and grants to hospitals and other healthcare providers to acquire information technology to improve patient safety and healthcare quality and to reduce adverse events. It also would amend a previous regulation to require a unique product identifier on packaging for drug or biological products subject to FDA regulation.

Centers For Medicare & Medicaid Services

CMS is also involved in patient safety. Effective Mar. 25, 2003, under the Medicare Conditions of Participation (CoP), hospitals must develop and implement a quality improvement program (QAPI) that will identify patient safety issues and reduce medical errors. The rule states that hospitals must:

- Establish, implement, maintain and evaluate a QAPI program
- Have a QAPI program that reflects the complexity of its organization/services
- Have a QAPI program that is hospital-wide and focuses on maximizing quality-of-care outcomes
- Include preventive measures that foster patient safety, such as reducing medical errors

Additionally, in concert with HHS Secretary Tommy Thompson's initiative to increase the use of information technology in healthcare, the Medicare rule allows hospitals to implement IT programs as part of their QAPI program.

Food & Drug Administration

In recent years, the FDA has focused on healthcare IT, primarily transfusion medicine software, but is now expanding into patient safety. The agency recently proposed two rules in this regard.

One—"Bar Code Label Requirements for Human Drug Products and Blood"—is expected to be finalized this year. It would provide bar-coding standards, requiring bar codes on all prescription drugs, over-the-counter

drugs packaged for hospital use and vaccines, as well as blood and blood components.

The other proposed rule—"Safety Reporting Requirements for Human Drug and Biological Products"—lists new requirements for reporting errors to the FDA, including all medication errors and all serious adverse reactions to blood and blood products.

Leapfrog Group

Spurred by the rising costs of providing medical benefits to employees in the private sector, the Leapfrog Group is attempting to motivate healthcare providers to implement improved safety standards, thereby reducing costs.

Leapfrog is a Washington, DC-based organization founded by the Business Roundtable, a national association of Fortune 500 CEOs. It was created to improve patient safety by mobilizing employer purchasing power to initiate breakthrough healthcare safety improvements and to provide consumers with information that would empower them to make more informed healthcare choices.

Leapfrog collects voluntary hospital survey data in order to develop respected industry standards. By publicizing provider safety performance data and economic sanctions, the group hopes to drive organizational improvements. The first three measures and standards on which Leapfrog has chosen to focus include:

- **Computerized Physician Order Entry (CPOE):** These systems can reduce or eliminate errors caused by handwritten prescriptions and provide alerts grounded on rules-based logic.
- **Evidence-Based Hospital Referrals (EHR):** For certain high-risk procedures and treatments, patients who go to hospitals that frequently perform these procedures/treatments or have demonstrated a good record of patient outcomes, have the best chance of surviving and successfully recovering. Patients should be guided to the hospitals and clinical teams that are more likely to produce better outcomes, according to the Leapfrog Group. This standard only applies to hospitals in metropolitan areas.
- **ICU Physician Staffing (IPS):** Adequate staffing of intensive care units with physicians who have credentials in critical care medicine has been shown to reduce the risk of patients dying in the ICU by more than 10%.

Patient Safety Compliance Programs

The HHS Inspector General has recommended that all healthcare institutions adopt a patient safety compliance program. The IG's Office has established a generic compliance program model for hospitals, with flexibility to tailor patient safety efforts to the hospital's specific requirements and unique philosophy/environment.

The patient safety compliance officer (CO) is critical to the overall success of a patient safety program. He or she must be highly visible to the governing body of the institution, have its support and enjoy the independence necessary to carry out the mandate. Employees should be encouraged to take any medical error, fraud or abuse concern directly to the CO. The Patient Safety Office of Compliance should be sufficiently staffed to address a multitude of patient safety issues.

It is common practice for healthcare facilities to establish a Patient Safety Compliance Steering Committee to guide and monitor their overall program. The patient safety CO is the conduit between a facility's governing body and the committee. This committee should be composed of at least one senior-level executive and at least one member of the entity's board of directors. Executive involvement and commitment are necessary to ensure that the program is taken seriously by all staff at all levels.

The patient safety compliance staff should include a representative from the information systems (IS) department, since most hospitals have computer clinical-alert systems to track clinical patient care. These applications can detail the number and type of physician orders, which doctor ordered the tests and the outcomes of the care provided. Typically, IS staff are the most familiar with the information accessible through information technology and can provide insights for staff consideration.

Both the patient safety CO and the Compliance Steering Committee should operate under written guidelines established by the entity's governing body. Their charter should grant sufficient authority to personnel to exercise their compliance function. The charter should further protect the compliance function from attempts to interfere with its independence.

Patient safety compliance training and education should be woven throughout the healthcare organization. It should be interactive, geared to practical application, and employees must be involved in developing the curriculum. Individuals should be encouraged to discuss the types of patient safety dilemmas most frequently encountered. Training should cover the entity's code of ethics and be formally recorded. Compliance programs should emphasize informal training continually throughout the year—for example, through a monthly newsletter that highlights such topics as updates on JCAHO standards, progress toward improving patient safety and important legal cases.

Training and education become more relevant to employees when they understand the impact of medical errors on the organization, which can be held responsible for the mistakes of a single employee. This liability can result in exclusion from Medicare, Medicaid and/or other federal healthcare programs.

Patient safety compliance programs must be periodically audited to ensure continued success. External audits provide increased objectivity and independence. Employee training and education should ensure that current, accurate information is being provided. The work of the patient safety CO and the Compliance Steering Committee should be monitored to assess their effectiveness. Audit results should be presented to senior management who have the responsibility to support recommended corrective actions.

The results of any independent compliance audits will likely be accessible to government investigators. This can be avoided by assigning compliance program review responsibility to outside legal counsel. However, attempts to invoke attorney-client privilege to shield compliance program records are likely to meet with extreme government opposition.

A patient safety compliance program does not immunize an institution from illegal conduct. The program can actually aggravate an institution's liability when medical errors occur, because it can show a lack of diligence. The real program benefit is minimizing the possibility of such conduct. Achieving this objective requires developing a culture committed to ethical conduct.

Use Of Information Technology

A common theme throughout patient safety programs is the promotion of IT to improve patient safety and reduce medical errors. Many facilities today lack integrated systems equipped to detect and correct errors before they occur. Patient safety COs should determine if there is a need for workflow process redesign in conjunction with the implementation of new technology in order to address the root causes of errors. They must assess if the technology can integrate data from various source systems, with adequate integrated decision-support capabilities such as reminders, suggestions/guidance and alerts at the time the order is placed (synchronous alerting).

Many systems can capture results information, providing analysis, trending and graphical displays which can assist in meeting internal and external reporting requirements. Also important are alerting capabilities after the order is placed (asynchronous alerting). Asynchronous alerting systems have the ability to monitor results and other clinical activities and to generate appropriate real-time alerts via wireless devices, e-mail, printers and fax machines. Alerts must be tailored to each clinician's workflow philosophy and provide the right information at the right time to make the appropriate decisions and must be adaptable as patient safety needs and requirements change.

Though a public outcry for a focused effort to reduce medical errors and improve patient safety has yet to happen, positive steps are underway and change is imminent. The dedication of the many legislative/governmental, regulatory and private-sector entities in creating safety guidelines and a dedication to compliance by healthcare providers are expected to lower the startling number of deaths cited in the original IOM report. And though the report was correct that "To Err is Human," it failed to mention other essential human traits: To learn, to change, to improve, to advance.

Dawn Kirschenman and Gay Fright can be reached at Misys Healthcare Systems, 4801 E. Broadway Blvd., Tucson AZ 85711-3609. Tel: 520-570-2000. E-mail: Dawn.Kirschenman @misyshealthcare.com and gayfright@misyshealthcare.com.

Dina Ross

HIPAA Security Contract, *from p. 1*

or outsource it and hire a security consultant," says Ross. This decision will depend largely on whether you have sufficient internal resources to implement the rule yourself, she adds.

Covered entities that decide to hire a security consultant should develop a request-for-proposal or request-for-information. This will "force you to sit down, put pen to paper and work through what you really need," she says. You should consider the consultant's experience with security issues, its financial stability and its reliance on subcontractors as well.

What To Keep In Mind

Once you select a consultant, you'll enter a contracting phase during which you'll establish expectations, determine payment and decide how the contract will end. Among the major considerations for this phase, she says, are these:

- ***Forms.*** While the consultant is likely to present you with a standard contract and express reluctance to deviate from it, "everything is negotiable." Don't be afraid to insist on modifications or amendments to ensure that your needs are met.
- ***Negotiation process.*** Get your firm's legal counsel involved early in this process. Also, delegate authority and establish a clear negotiation schedule.
- ***Scope of services.*** It's imperative that the contract clearly defines "scope of service." Use specific references from provisions of the security rule, specify the methodology for risk assessment, specify milestones and deliverables, and set commencement and completion dates. You should also avoid "scope creep" by including change control provisions and project management specifications. Also, beware of attempts by the consultant to shift obligations to you through use of "assumptions" and "client responsibilities," Ross cautions.
- ***Charges.*** Hourly payment is fairly common in consulting, but there are ways you can limit the risk of being overcharged. One way is to condition payment on achievement of certain milestones (instead of dates) or to specify that payment is "not to exceed" a set amount. Consultants, however, may be reluctant to agree to such terms, she admits. A consultant may be more likely to agree to a "sliding discount." Under this arrangement, both parties establish a point beyond which the client begins receiving a discount on the hourly rate. "At some point, it's got to start costing the consultant to keep its people there."
- ***Indemnification.*** The consultant's contract will likely include language stating that you, the client, indemnify the consultant for all claims relating to engagement of the consultant and for all claims resulting from use, possession or reliance on the consultant's advice, Ross notes. "These should be deleted." Any indemnification should be mutual and should cover intellectual property claims, breaches of confidentiality (including business associate obligations), property damage and personal injury.
- ***Deliverables.*** The final work product should be clearly described. Limitations on disclosure related to the work product should not apply to auditors, attorneys or future consultants. "Future consultants might be the sticking point, since your consultant might be concerned that you'll be sharing 'state secrets' and their methodology with someone else," she says. "You can work around that or limit it, but at the end of the day, you want to be able to take the work product you paid for and use it as you see fit." While the consultant may insist on owning the work product, you should ensure that you have sufficient license rights, she adds. It's important, however, that you place limits on any unique or proprietary information to prevent the consultant from divulging it.
- ***Consultant's software.*** If the consultant uses its own software, make sure you have the right to use it once the contract has terminated. You might even consider having a "source code escrow" that allows you to get the software source code in the event of bankruptcy or change of control at the consultant company.
- ***Warranties.*** While a consultant will not likely provide a warranty on its service, it should at least be willing to warrant that its services will be delivered in a "timely, competent and workmanlike manner," says Ross. Avoid "sole remedy" language that limits your ability to pursue monetary damages if necessary.
- ***Exit strategies.*** Establish clear guidelines

as to when the contract will end. Ross advises including language stating that the client may terminate the contract at its "convenience." While this may entail a payoff fee, it may save you additional legal fees and angst if the deal ends badly. You should also include a provision stating that the arrangement may be terminated if there is a "breach" of the contract.

Resource

❖ Dina Ross: 312-984-6477

HIPAA Security Standards Matrix

Standard and Section	*Implementation Specification* *(R=Required, A=Addressable)*
Administrative Safeguards	
Security Management Process (164.308(a)(1))	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility (164.308(a)(2))	(R)
Workforce Security (164.308(a)(3))	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)
Information Access Management (164.308(a)(4))	Isolating Healthcare Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training (164.308(a)(5))	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures (164.308(a)(6))	Response and reporting (R)
Contingency Plan (164.308(a)(7))	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Application and Data Criticality Analysis (A)
Evaluation (164.308(a)(8))	(R)
Business Association Contracts and Other Arrangement (164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards	
Facility Access Controls (164.310(a)(1))	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use (164.310(b))	(R)
Workstation Security (164.310(c))	(R)
Device and Media Controls (164.310(d)(1))	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards	
Access Control (164.312(a)(1))	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls (164.312(b))	(R)
Integrity (164.312(c)(1))	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication (164.312(d))	(R)
Transmission Security (164.312(e)(1))	Integrity Controls (A) Encryption (A)

Source: McDermott, Will & Emery

DOJ Okays $631 Million HCA Settlement

When added to civil and criminal settlements reached in 2000, the settlement just announced will bring the government's total recoveries from HCA to about $1.7 billion

The U. S. Department of Justice has approved a settlement agreement under which HCA Inc. (Nashville, TN) will pay $631 million to the United States to resolve allegations of healthcare fraud. HCA, the nation's largest for-profit hospital chain, reached a tentative settlement last December, but the deal had to be approved by officials at Justice.

The final accord resolves allegations that the company overcharged the government in its cost reports, made illegal payments to physicians in exchange for referrals of patients and overcharged Medicare and Medicaid in connection with HCA's agreements for management of its wound care facilities.

HCA will pay an additional sum—$250 million—to the Centers for Medicare & Medicaid Services to resolve its administrative liability.

Sen. Charles Grassley (R-IA), a vocal critic of the settlement agreement, says he will meet with representatives of the Justice Department and the HHS Office of Inspector General about concerns he raised in an Apr. 30 letter to Attorney General John Ashcroft and HHS Secretary Tommy Thompson. Grassley is concerned that the settlement does not consider 2,600 cost reports that the government "apparently" never reviewed and, consequently, may not reflect the actual amount that HCA may have overcharged.

Most Part A Providers Expect Timely HIPAA Compliance

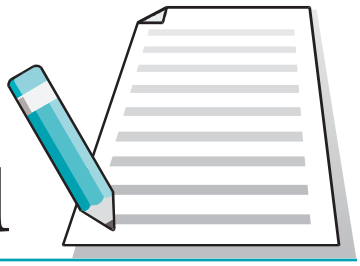
Most Medicare Part A providers expect to comply with federal requirements for electronic transactions and code sets by the Oct. 16, 2003, deadline, according to a survey released in May by the HHS Office of Inspector General. The requirements are set forth in a final rule implementing provisions of HIPAA—the Health Insurance Portability & Accountability Act.

The OIG survey, "HIPAA Readiness: Administrative Simplification for Medicare Part A Providers," found that 74% of all providers were ready to comply with the standards at the time they responded and that 96% of Part A providers expect to comply by the deadline.

Despite respondents' stated belief that they will meet the deadline, fewer than 30% had begun testing when the survey was conducted between Nov. 26, 2002, and Mar. 24, 2003, though 90% said they had a testing strategy. Covered entities were supposed to begin testing their systems by Apr. 16.

"Providers are using expert resources outside their organization to help implement HIPAA standards and code sets," the survey report noted. "Eighty-one percent stated they had turned to their professional associations for information to assist them in developing implementation strategies. Approximately 84% of all providers are using system vendors as part of their compliance strategies."

For the Record



If a physician receives a subpoena from a court to provide a patient's records, does the subpoena "trump" the medical privacy protections under HIPAA—the Health Insurance Portability & Accountability Act—or must the doctor obtain authorization from the patient before releasing the records?

Section 164.512 of the HIPAA privacy regulations provides that a covered entity may use or disclose protected health information without the written consent or authorization of the individual in response to a subpoena, discovery request or other lawful process if the covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to:

- Ensure that the individual in question has been given notice of the request, or
- Secure a qualified protective order.

Under HIPAA, a covered entity receives satisfactory assurances if it receives a written statement and accompanying documentation demonstrating that:

- A good-faith attempt has been made to provide written notice to the individual,
- The notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection and
- Either no objections were filed or all objections filed have been resolved.

Cost-Sharing Waiver Okay: A nonprofit ambulance company may collect fixed annual subscription fees from beneficiaries in lieu of Medicare Part B cost-sharing amounts without violating the anti-kickback statute and risking administrative penalties, said the HHS OIG in a May 28 advisory opinion (No. 03-11). The arrangement typically would be a kickback violation because cost-sharing waivers could potentially be used to induce or reward referrals, according to the advisory opinion; however, the subscription fees exceed the cost-sharing amounts that beneficiaries would be expected to pay, thus limiting the risk of abuse. The advisory opinion is posted at *http://oig.hhs.gov/fraud/advisoryopinions/opinions.html*.

Another PATH Settlement: Philadelphia-based Albert Einstein Healthcare Network has agreed to pay just under $2 million to resolve allegations that it billed Medicare improperly for inpatient services between January 1995 and June 1996, federal law enforcement officials said May 28. The civil settlement culminates an investigation and audit by the HHS OIG under its Physicians at Teaching Hospitals (PATH) initiative. The government alleged that Einstein submitted claims for inpatient services that were represented as having been personally performed by Einstein physicians when it lacked sufficient documentary evidence to support the claims. The government also alleged that Einstein submitted claims for services rendered by its physicians that were improperly upcoded. Einstein denies the government's allegations. The text of the settlement is posted at *http://www.usao-edpa.com/Pr/2003/may/einstein.html*.

Transfer Overpayments: Medicare paid an estimated $61 million in excessive payments to hospitals in fiscal 2000 because of incorrect coding on claims for discharges that were subject to the post-acute care transfer policy, the HHS OIG said in a May 19 report. The OIG determined from a sampling of claims that the coding errors occurred because the Centers for Medicare & Medicaid Services did not have controls or edits to detect the excessive payments. It recommended that CMS establish a mechanism within the Common Working File that compares inpatient claims with subsequent post-acute care claims and that CMS instruct fiscal intermediaries to recover the actual $736,543 identified in the sampling. The report *is posted at http://oig.hhs.gov/oas/reports/region4/40207005.pdf*.

G-2 Compliance Report Subscription Order or Renewal Form

Subscription Service includes 10 issues of the *G-2 Compliance Report*, 4 quarterly Critical Issue Compliance Audiocassettes, the G-2 Compliance Resource Manual, and Compliance FastTrak Fax Alerts, plus exclusive savings on G-2 compliance seminars and publications

❑ ***YES***, enter my one-year subscription to the ***G-2 Compliance Report*** at the regular rate of $399/yr.

or

❑ ***YES***, as a current subscriber to the *National Intelligence Report*, *Laboratory Industry Report* and/or *Diagnostic Testing & Technology Report*, enter my subscription to the ***G-2 Compliance Report*** at the special reduced rate of $319/yr, $80 off the regular rate.

Please Choose One:

❑ Check Enclosed (payable to Washington G-2 Reports)

❑ American Express ❑ VISA ❑ MasterCard

Card # _____ Exp. Date _____

Cardholder's Signature _____

Name As Appears On Card _____

Ordered by:

Name _____

Title _____

Company/Institution _____

Address _____

City _____ State _____ Zip _____

Phone _____ Fax _____

e-mail address: _____

MAIL TO: Washington G-2 Reports, 29 W. 35th St., 5th Floor, New York NY 10001-2299. Or call 212-629-3679 and order via credit card or fax order to 212-564-0465 6-7/03

G-2 Compliance Report (ISSN 1524-0304). © 2003 Washington G-2 Reports, 1111 14th St, NW, Suite 500, Washington DC 20005-5663.
Tel: (202) 789-1034. Fax: (202) 289-4062. Order Line: (212) 629-3679. Website: www.g2reports.com.