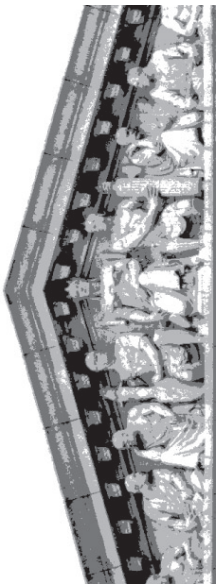

G-2 Compliance Report

WASHINGTON G-2 REPORTS

Vol. V, No. 3, March 2003

For Hospitals, Laboratories and Physician Practices

Final HIPAA Security Rule Helps Clear Confusion
Standards Mostly Mesh With Privacy Reg

To the relief of many in the healthcare industry, the just-released final HIPAA security rule appears to settle some of the confusion over how its standards will align with the final HIPAA medical privacy standards scheduled to take effect this Apr. 14.

Security and privacy are mutually dependent functions, but the proposed security rule, issued in 1998, did not make clear how the two would interact, a significant worry to healthcare providers and other entities subject to the Health Insurance Portability & Accountability Act (HIPAA), including health plans and health clearinghouses.

The final security rule, which appeared in the Feb. 20 *Federal Register*, clarifies to some extent how the two sets of standards work together, and it aligns much of the proposed security rule's terminology and definitions with those in the privacy regulation, thus facilitating compliance *(see Perspectives, pp. 5-8)*.

➔ *p. 10*

Validating CLIA Moderate Complexity Tests
Labs Should Consult With Manufacturers

Laboratories performing tests classified as moderate complexity under CLIA (Clinical Laboratory Improvement Amendments) should begin taking steps now to prepare for the validation that will be required when the new CLIA quality control regulation takes effect next month, experts advise.

As of Apr. 24, all labs that perform unmodified, FDA-approved moderate complexity tests will have to validate the accuracy of such tests introduced thereafter prior to use in the testing of patient specimens and the reporting of test results. Previously, these labs had to meet minimal QC requirements for such tests under a special phase-in period that expired last Dec. 31.

Though the new validation requirement goes into effect next month, these labs will have one full CLIA survey cycle to achieve compliance, which should give them plenty of time to learn how to validate tests if they don't already know, says Judy Yost, director of the division of laboratory services at the Centers for Medicare & Medicaid Services.

"Labs will have two years to come into full compliance," Yost tells *G-2 Compliance Report*. "We're not going to hold anyone accountable in the beginning, but we felt it was important to get labs used to the idea that they will need to do some kind of validation."

➔ *p. 4*

Inside this issue

CBC Billing Perplexes Labs Under 2003 CPT Revisions

Is your laboratory billing correctly for complete blood counts (CBCs) that lead to manual differentials? You may be surprised at the answer—or lack of one.

At issue is how labs should bill Medicare when they perform a CBC with automated differential and, because of an aberrant result, a manual differential is then performed. In the past, labs would bill using code 85023. However, that code was deleted from the 2003 CPT update, which became effective Jan. 1.

Many labs are unsure whether they should bill 85025 (CBC with auto diff) or 85027 (the complete CBC, automated) plus 85007 (the manual diff). Experts differ on how the billing should be done, and the Centers for Medicare & Medicaid Services is evaluating the issue.

Two Views

According to coding consultant Joan Logue, head of Health Systems Concepts (Longwood, FL), when a physician specifically orders a CBC with a manual differential, the lab should bill 85027 (the complete CBC, automated) and 85007 (manual differential). However, when a physician specifically orders a CBC with automated differential, the lab should report 85025, even when the instrument flags the differential and the lab performs a manual differential in addition, she says.

Labs should not unbundle and bill the component tests 85027 and 85007 when an 85025 is ordered in order to obtain payment for the manual differential, Logue warns, noting that Medicare considers the reflex to the manual differential to be part of the steps necessary to complete the physician's order.

"The CCI (correct coding initiative) lists 85007 as a component test of 85025," she says. "If you have to perform the manual diff because of your testing protocol to fulfill the physician's order for the CBC and diff, then the manual differential is included in 85025. You have to bill what the physician orders, not what you decide to do."

However, Diana Voorhees, coding and compliance consultant and principal of DV & Associates (Salt Lake City, UT), believes the issue is more complex. If the CBC with automated differential produces questionable results, a verification process should occur next, she says. This usually includes a review of a manual smear (e.g., CPT 85008) to confirm the automated results. If the results are verified, the manual review is part of quality control and is bundled in the reported 85025.

But if the automated results for the differential are invalid (cannot be reported), there are no results and there is not a "true reflex" situation; thus, a manual differential must be performed to generate a report for the differential, Voorhees believes.

"In 2002, the coding would have been CPT 85023; this code is reflected as 85027 and 85007 in 2003," she says. "The manual differential is a necessary part of the testing ordered to report results. Not all labs assign codes on their requisition or allow physicians to determine the differential methodology."

Complicating the issue is the fact that labs would be paid more when billing Medicare for 85027 (capped nationally at $9.04) plus 85007 ($4.81) than they would have been paid under the deleted 85023 code ($11.84). By billing for both the complete CBC, automated, and the manual diff, labs will be paid more than $2 more for the same testing. Voorhees adds that in the past, labs received a dollar more for 85023 than for 85025. "Reimbursement was an issue last year and remains an issue this year," she notes.

The View At CMS

The new CPT codes for hemograms have created a number of issues for providers as well as payers such as Medicare, acknowledges a CMS spokesperson. "As of this time, CMS has not changed its policies regarding hemograms and differentials. If a hemogram with automated differential is ordered, the provider should bill 85025 even if the reflex manual differential is necessary to complete the ordered tests. CMS is continuing to evaluate this issue."

In the meantime, labs should establish clear procedures about how they bill for a manual differential when a CBC with auto differential is ordered, advises Voorhees. Thorough policies and careful documentation are always

the best line of defense. "This is something every lab has to look at," she says. "Procedures need to be spelled out and approved by the medical authorities at each facility. If you get questioned, you need to justify why you did it the way you did."

Resources

Joan Logue: 407-774-5291
Diana Voorhees: 801-272-3672

HHS Modifies Electronic Transactions/Code Sets Rule

The revised rule is posted at www.cms.gov/regulations/hipaa/cms0003-5/0003ofr2-10.pdf

On the same day that it published the final HIPAA security rule, the U.S. Department of Health & Human Services adopted changes to the electronic transactions/code sets rule it had previously promulgated in accord with HIPAA (the Health Insurance Portability & Accountability Act of 1996).

The changes, published in final form in the Feb. 20 *Federal Register*, combine two regulatory proposals unveiled on May 31 of last year *(GCR, Jun-Jul '02, p. 1)* and also modify a number of national standards adopted under HIPAA for electronic transactions and code sets. In making the revisions, HHS says it worked extensively with the Designated Standards Maintenance Organizations (DSMOs).

Specifically, the revised rule:

- Repeals the National Drug Code (NDC) as the standard medical data code set for reporting drugs and biologics in all non-retail pharmacy transactions.
- Adopts the proposed addenda to the implementation guides, with some technical revisions made in consultation with the DSMOs.
- Adopts, as the standard for payment and remittance advice, the Accredited Standards Committee (ASC) X12N 835 and, as the standard for the referral certification and authorization transaction, the National Council for Prescription Drug Programs (NCPDP) Telecommunications Version 5.1 and NCPDP Batch Version 1.1 Implementation Guides.

Hospitals Charged With Improper Lab Billings

The U.S. Department of Justice has filed civil suits against two Massachusetts hospitals for improperly billing Medicare for laboratory services to outpatients. The suits seek recovery of nearly half a million dollars in claims, plus interest.

Lahey Clinic Hospital and the University of Massachusetts Memorial Medical Center, both in Boston, are charged with two counts of improper billing of blood tests during the mid-1990s, according to U.S. attorney Michael Sullivan. The government is seeking to collect $311,000 from Lahey and $125,000 from Memorial Medical.

On the first count, the government alleges that Lahey and Memorial Medical billed for hematology indices, even though these indices were neither medically necessary to treat or diagnose the patient nor ordered by an attending physician. According to the government, physicians ordered, and hospitals performed, a complete blood count (CBC). The same blood analyzers that performed the CBCs also generated, as a byproduct, indices calculations. The hospitals allegedly billed Medicare for the CBCs, then separately billed the program for the indices.

On the second count, the government alleges that the hospitals performed a number of automated multichannel chemistry panels and individual tests on one blood analyzer for the same patient on the same date of service, but failed to "bundle" these panels or tests into a single charge for Medicare billing purposes. Instead, the hospitals "unbundled" the panels when billing Medicare, thus getting higher reimbursement.

The lawsuits stem from an investigation that resulted in a settlement in August 2000 with eight Massachusetts hospitals for similar billing practices. The government collected more than $1 million from those settlements. Since then, Medicare has banned indices billing and required local contractors to bundle automated tests (though labs may do so if they choose).

Resource

- Michael Sullivan: 617-748-3139

CMS estimates that implementing the new verification requirement for certain moderate complexity tests will cost between $28.3 million and $37.1 million in the first year and between $124.1 million and $162.5 million over the next five years

Validating CLIA Tests, *from p. 1*

Under the final CLIA QC rule *(GCR, Feb. '03, p. 1),* labs that perform an unmodified, FDA-cleared moderate complexity test must demonstrate performance specifications comparable to the test manufacturer's for accuracy, precision and reportable ranges. The lab director must decide the extent to which these specifications are verified, based on the method, testing conditions and personnel performing the tests.

In cases where a lab uses a test system for which the manufacturer does not provide performance specifications, labs must, before reporting patient test results, establish such specifications for the following performance characteristics: 1) accuracy, 2) precision, 3) analytical sensitivity, 4) analytical specificity, including interfering substances, 5) reportable range of test results for the test system, 6) reference intervals (normal ranges) and 7) any other performance characteristic required for test performance.

These new requirements are expected to affect about 17% (29,601) of the nation's CLIA-certified labs, estimate CMS and the Centers for Disease Control & Prevention. These include 22,720 Certificate of Compliance labs and 6,881 COLA-accredited labs, most of which are physician office labs (POLs).

"Do The Best You Can"

The final CLIA QC rule provides few specifics on how to validate a moderate complexity test, which could worry some labs, especially POLs, notes C. Anne Pontius, president of Laboratory Compliance Consultants (Raleigh, NC).

"The actual rule is very broad. It doesn't say exactly how many tests you have to run to meet the requirements, whereas the guidelines of the NCCLS (National Council for Clinical Laboratory Standards) might say that to establish reportable ranges, you have to run 100 tests. There's no way that a physician office lab will have the resources to do full-blown studies."

In fact, CMS does not expect these smaller labs to meet that level of validation, explains Yost. "We understand that it's not feasible for small labs to do 35 specimens and correlate results. Our advice at this point is to do the best you can. The intent of the requirement for moderate complexity test validation is that labs do something to show that tests work before they report results, so if they can split a sample and send some out and compare results, we would be happy."

While CLIA surveyors may cite a lab for a deficiency during the first survey cycle following implementation of the new requirement, CMS will not take any enforcement action against the lab (assuming it complies in other regulated areas), but will provide technical assistance and education to help the lab achieve compliance, Yost adds.

"Work With Manufacturers"

CMS plans to publish more specific guidance on how to perform test validation in late summer or early fall. In the meantime, both Yost and Pontius advise labs to work with test and equipment manufacturers on validation procedures.

"You need to make some attempt to verify these parameters and do this in conjunction with the manufacturer," says Pontius. "Ask the manufacturer what it considers the minimum needed for verification and follow that advice."

Labs should ensure that office personnel are involved in the validation process, she adds. It is not enough to have the manufacturer perform the validation in the presence of staff and leave the appropriate documentation. "CMS wants to make sure that the manufacturer and the staff do it together, because the whole purpose is to teach staff how to identify problems within the system," she explains.

Pontius also advises labs that are in the process of purchasing new tests and equipment to ensure that these are in place and working by the effective date of the QC rule, since only tests introduced after that date must be verified by the lab. "I would write into a contract that if the equipment is not up and running by Apr. 24, then the manufacturer has to pay for all the materials needed to do the accuracy, precision and verification," she tells *GCR.*

Resources

- Anne Pontius: 919-859-3793
- Judy Yost: 410-786-3407

COMPLIANCE PERSPECTIVES

Ways To Think About Security Under New HIPAA Rule

Richard D. Marks, Esq., is a partner in the Washington, DC office of Davis Wright Tremaine LLP

Paul T. Smith, Esq., is a partner in the firm's San Francisco office

While the new security rule under the Health Insurance Portability & Accountability Act (HIPAA) goes into effect Apr. 21, 2005, the effective date, some two years away, tells only part of the story. In less than two months, the "mini-security rule" in the HIPAA *privacy* regulation takes effect. It requires HIPAA-covered entities (healthcare providers, health plans and health clearinghouses) and their business associates, as of Apr. 14, 2003, to implement "appropriate administrative, technical and physical safeguards" for protected health information in all forms, non-electronic and electronic. It's likely that these "appropriate safeguards" will in part be determined by referring to the general principles (if not all the specific requirements) of the final security rule. From this perspective, the first impact of this new rule is almost immediate.

The rule fulfills the oft-repeated promise by the U.S. Department of Health & Human Services to mesh security and privacy standards under HIPAA. It discards much of the terminology in the proposed security rule in favor of definitions in common with the final privacy rule. For example, requirements for the "chain-of-trust" agreement under the proposed rule are now made additional requirements to "business associate" contracts required by the privacy rule.

Some changes in terminology were made simply for consistency with the privacy rule. Others reflect a shift in substance, such as the change from security "certification" to "evaluation," or the shift from "information access control" to "information access management," a broader concept. Other modifications introduce a new concept, approach or new emphasis, such as the provisions for "media re-use procedures."

Generally speaking, the final security rule offers less detail and more generic guidance, in the sense of high-level direction, about how HIPAA-covered entities and their business associates should go about implementing security. As HHS says, "We have focused more on what needs to be done and less on how it should be accomplished."

This means that the new rule contains less a series of checklists and more a description of principles for each covered entity and business associate to evaluate and apply, based on the entity's specific situation. One benefit to this approach, as a general matter, is less regulatory risk through the enforcement process. Other risks remain, however, because of the new rule's demands on covered entities to exercise constant vigilance and apply prudent judgment about security to changing circumstances. These are familiar litigation risk management issues.

The new rule's scope is narrowed to protected health information (PHI) in electronic form only. Consequently, many details of implementing the security rule may not apply to PHI in non-electronic form. However, the government emphasizes that the privacy rule does apply to PHI in *any* form. The reader should remember the "mini-security rule" (45 CFR 164.530(c)), discussed above. It requires that "appropriate" security be applied to all PHI in any event, whether or not the security rule itself applies.

Structural Elements

The final security rule uses a "Security Standards Matrix" to lay out standards and implementation specifications. The latter can be either "required" (R) or "addressable" (A). The matrix, in Appendix A to the rule, shows by an "R" or an "A" whether a particular implementation specification is required or addressable and lists the section of the secu-

No Safe Harbor

The final HIPAA security rule offers no safe harbor to covered entities, business associates or the people who make security decisions for them. Rather, whether security countermeasures are good enough to "ensure" the confidentiality, integrity and availability of protected health information and protect it from "any" hazard one could reasonably anticipate, is likely to be judged retroactively. Results and the documentation of decisions will both be important.

These considerations apply both to HHS's regulatory enforcement of security and privacy, and to covered entities' and business associates' management of litigation risk. Because the rules are based on judgments involved in risk assessment and risk management, and on the effective implementation of the security management process, there is inherent exposure to legal liability. This cannot be eliminated, and the new rule does not attempt to do so.

rity rule where the standards and implementation specifications are found. The standards are grouped under three headings: Administrative Safeguards, Physical Safeguards and Technical Safeguards.

Essentially, a standard explains what must be done, and implementation specifications explain how to do it. If HHS believes that an implementation specification is one of many options, none of which by itself is essential, then it will label that specification "addressable." If HHS sees the specification as essential, it will be "required."

In some cases, a standard is sufficiently self-contained so that the means of its implementation are explicit or implicit, without the need for any implementation specifications. For example, "assigned security responsibility" (164.308(a)(2)) and "workstation use" (164.310(b)) stand alone and do not include any specifications.

Thinking About Security

The standards and implementation specifications are integral to how HHS wants covered entities and their business associates to think about security. The preamble reflects HHS's recognition (gleaned from comments on the proposed rule) that many in the healthcare industry found security perplexing.

The place to start thinking about security under the new rule, says HHS, is Section 164.306. This section is the heart of the new rule and tracks that part of the HIPAA statute which governs security standards and safeguards (42 USC 1320d-2). Covered entities must meet four security requirements specified in Section 164.306(a):

(1) Ensure the confidentiality, integrity and availability of all electronic PHI the covered entity creates, receives, maintains or transmits.
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
(4) Ensure compliance . . . by its workforce.

Section 164.306(b) specifically calls for a flexible approach: "Covered entities may use any security measures that allow [them] to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." The rule allows covered entities to factor in cost, size, complexity, technical infrastructure, other capabilities and the likelihood and seriousness ("criticality") of potential security risks.

Section 164.306(c) specifies that covered entities accomplish all this by reference to the standards and their associated implementation specifications, whether required or addressable. If the standard has no implementation specifications, it can and must be implemented as the standard itself specifies. If there are required implementation specifications, then the covered entity must do what the specifications demand.

However, there is significant flexibility in approach because so many of the implementation specifications are addressable, not required. A covered entity must assess whether each addressable specification is reasonable and appropriate for its unique situation. Then it has choices. If the specification is reasonable and appropriate, it "must" be implemented. If not reasonable and appropriate, the entity must either implement another equivalent measure that is reasonable and appropriate or, if the standard can be met in some other way, choose not to implement the specification or any equivalent specification. The covered entity must document the reasons for its choice.

Risk Assessment, Risk Management

The preamble to the final security rule explains that: "The administrative, physical, and technical safeguards a covered entity employs must be reasonable and appropriate to accomplish the tasks outlined in paragraphs (1)

through (4) of §164.306(a)." The way a covered entity knows what measures are reasonable and appropriate to achieve each of the listed tasks is via a two-step process mandated in the rule. First, assess the security risks faced. Then, implement countermeasures proportional to those risks and manage countermeasures to keep up with new or increased risks.

HHS explains it this way: "An entity's risk analysis and risk management measures required by §164.308(a)(1) must be designed to lead to the implementation of security measures that will comply with §164.306(a)." Whether particular measures comply will be determined by their effectiveness in "ensuring" the confidentiality, integrity and availability of PHI and in protecting PHI against "any reasonably anticipated threat or hazard." By the way it has written Section 164.306 and explained it in the preamble, HHS has set a high standard for security and narrowed legal arguments about how to interpret the HIPAA statute's language about safeguards.

HHS refers several times to guides published by NIST—the National Institute of Standards and Technology—as an aid in risk assessment and security management (discussed below). The NIST "800 Series" publications are important as practical guides that expand on HHS's explanation of steps to follow, and criteria to use, when assessing risk and managing security implementation. The guides also will be important references in HHS's enforcement of the security rule and in other litigation over security issues.

The preamble's discussion of risk assessment and risk management will assist covered entities in understanding what they should do to achieve an appropriate level of security, how to make decisions about doing it, and how to document it. Documentation will be a critical element in justifying a covered entity's approach to its security needs and the countermeasures it selects to meet them.

Security Management Process

The new rule requires covered entities and business associates to manage security processes assiduously. There is new emphasis, for example, on an entity's ability to detect an intrusion (such as a hacker attack) and respond quickly and effectively with countermeasures. This is known as "incident response." This and similar security management requirements will likely lead to integration of security processes and technology that is not yet common in healthcare. The expense of these precautions may well fall sooner and more heavily on larger healthcare organizations, because of the rule's emphasis on scalability. Training is one aspect of security management, and the new rule states that security training must be given to a covered entity's entire workforce, not just those who come in contact with PHI.

Business Associate Contracts: *Security Aspects*

One of the requirements of the proposed security rule was a "chain-of-trust partner agreement," by which two parties agree to exchange electronic data and protect it in the course of transmission. The goal was to ensure security at all points in the transmission, and it would have been required for all electronic transmissions of PHI.

The privacy rule has a different requirement, the "business associate contract." This is an agreement that a covered entity must obtain from contractors—called business associates—who assist the covered entity with payment or operations, and who have access to its PHI. Such a contract is not universally required for exchanges of health information—for example, a provider needs one to disclose health

A New Take On Technology?

The final HIPAA security rule only sets out a process for decision-making. It does not make the decisions nor prescribe any particular technology. Indeed, the preamble is determinedly and explicitly technology-neutral. This is true for issues covering everything from how to protect workstations to whether encryption is appropriate in any given situation. Some examples are worth noting because they have been the subject of so much discussion since the proposed security rule appeared in 1998:

- The preamble to the rule explains which kinds of fax processes are "electronic" and which aren't. The rationale, we predict, will continue to be a source of controversy and bemusement. Generally speaking, paper-to-paper (old-style) faxes are not electronic, and computer faxes are electronic.
- Voice (*i.e.*, good old) telephone is not electronic.
- The rule disavows a distinction between data that moves internally within or externally to an organization. This is likely to lead many covered entities to assess the risks associated with their internal networks in a new light.
- The much-criticized proposal that workstations have required automatic log-off is a thing of the past. Workstation protection is now much more flexible in concept.

information to a clearinghouse, but not to a health plan, because the clearinghouse is viewed as assisting the provider with payment, but the health plan is acting independently. Similarly, disclosures to providers for treatment do not require business associate contracts.

Observers have been interested to see how the final security rule would coordinate these differing requirements. It does so by abandoning the chain-of-trust partner agreement as a legal requirement. Instead, it requires covered entities to have agreements with business associates who create, receive, maintain or transmit electronic PHI on the covered entity's behalf. These agreements must contain assurances from the business associate that it will appropriately safeguard the information.

The security rule sets forth the required assurances. They are a subset of provisions required by the privacy rule, focused on electronic information. The business associate contract must require the business associate to:

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the covered entity's electronic PHI.
- Ensure that its agents and the subcontractors to which it provides the information do the same.
- Report to the covered entity any security incident of which it becomes aware.

The contract must also authorize termination if the covered entity determines that the business associate has violated a material term.

The security rule adopts the privacy rule's definition of "business associate." It also echoes the privacy rule's exceptions to the contract requirement for disclosures to providers for treatment, exchanges of information between government entities, and exchanges between group health plans and their sponsors. Interestingly, the security rule does not dispense with business associate contracts for covered entities participating in an organized healthcare arrangement, as the privacy rule does.

Likewise, the standard of liability is the same as under the privacy rule—a covered entity would not be liable for breaches by its business associate unless it knew of a pattern of activity or practice in violation of the agreement, and failed to take appropriate measures. Otherwise, covered entities that transmit data electronically will not be responsible for the recipient's security implementation.

The requirement that the business associate report to the covered entity any security incident of which it becomes aware makes it likely that covered entities will know about most, if not all, incidents. (The new rule discards the term security "breach.") Further, security protocols require close coordination, so it is unlikely that covered entities and business associates will be able to maintain the business process or technical process separation that the new security rule seems to envision. We will need experience under the new rule before these apparent contradictions can be evaluated.

In every case in which the security rule would require a business associate contract, the privacy rule would too. Accordingly, the requirements of the security rule will most likely be implemented as additional provisions to the standard contract for business associates that deal with a covered entity's electronic PHI.

Unlike the proposed chain-of-trust partner agreement, the business associate contract does not relate to the security of the data transmission itself, but rather to the security of data in the hands of the business associate. Moreover, many electronic transmissions of health information will not be subject to the business associate rule at all, such as transmissions between providers and health plans for payment. Neither the privacy rule nor the security rule has any requirement for a contract between participants in transmissions such as these.

However, the privacy rule in a general way, and the security rule more specifically, will require covered entities to ensure the security of electronic data transmissions, whether or not the recipient is a business associate. And participants in electronic data interchange will still need to agree on communications and security protocols, so trading partner agreements are likely to continue to be recommended practice. Prudence will argue for security risk analysis and ongoing risk management in the negotiation and implementation of these agreements.

Richard D. Marks can be reached at Davis Wright Tremaine LLP, 1500 K Street NW, Suite 450, Washington DC 20005-1272. Tel: 202-508-6611. E-mail: richardmarks@dwt.com

Paul T. Smith can be reached at Davis Wright Tremaine LLP, One Embarcadero Center, Suite 600, San Francisco CA 94111-3611. Tel: 415-276-6532. E-mail: paulsmith@dwt.com

New Corporate Fraud Law Likely To Impact Healthcare Providers

Additional information about the Sarbanes-Oxley Act, including a copy of Thompson's letter to federal prosecutors, is online at www.usdoj.gov/dag/cftf/

Healthcare providers can expect to see stepped-up enforcement against fraud and abuse in the coming year, due largely to passage last year of the Sarbanes-Oxley Act, a federal law that targets corporate fraud.

Armed with the new law, federal prosecutors and regulators are more likely to take a more hard-line approach to violators than they have in the past, predicts attorney John Bentivoglio with Arnold & Porter (Washington, DC). He spoke at the 6th Annual National Healthcare Compliance Congress, held Feb. 6-7 in Washington, DC.

Federal enforcement agencies are focusing in particular on obstruction of justice. "The government takes very, very seriously how companies respond to investigations," Bentivoglio pointed out. He advised healthcare entities to be more cautious in deciding what documents they destroy—and for what reasons.

The Sarbanes-Oxley Act, passed in response to corporate scandals such as WorldCom, Enron, etc., enhances penalties for obstruction of justice. Many provisions apply to privately held companies in the same way that they do to publicly traded entities.

The Act also has led to tougher sentencing guidelines and revised Department of Justice fraud directives. The U.S. Sentencing Commission on Jan. 8 announced it has approved significant increases in penalties for corporate fraud, including longer prison terms for those convicted of obstruction of justice. The strengthened penalties became effective Jan. 25.

Further, in a Jan. 20 letter to federal prosecutors, U.S. deputy attorney general Larry Thompson issued revised guidelines for determining whether to bring charges against business organizations. Among the factors that prosecutors should consider, he noted, was whether companies attempted to impede an investigation or otherwise obstruct justice. However, prosecutors should also weigh whether companies voluntarily disclosed wrongdoing and their willingness to cooperate with investigators, he said.

Thompson directed prosecutors to look at whether organizations had existing compliance programs and whether they were willing to improve those programs (the mere existence of a compliance program would not be grounds for leniency). Bentivoglio echoed the revised guidance from Justice, saying a well-written code of conduct or compliance program manual does not constitute an effective compliance program. The government wants more tangible evidence that efforts are being made to prevent fraud, he said.

More Compliance Directives On OIG's Project List For 2003

The HHS Office of Inspector General plans to issue a compliance resource guide for boards of directors of healthcare organizations sometime this year, IG Janet Rehnquist announced Feb. 6 at the 6th Annual National Healthcare Compliance Congress, held in Washington, DC.

Rehnquist said her office is working on a questionnaire-style guide that these corporate boards could use to help assess their compliance risk areas, including new accountability requirements for private and publicly held companies under the Sarbanes-Oxley Act of 2002. The guide should be ready in the spring, she said.

In addition, new compliance program guidance should be released in the near future. Final guidance for the ambulance industry will be out in the "next few weeks," Rehnquist noted, followed in the spring by final guidance for pharmaceutical manufacturers. Her office is revisiting previously issued compliance program guidance to various healthcare sectors to ensure that it is up-to-date, she said, and also continues to investigate cases involving medically unnecessary services.

Rehnquist intends to commit additional resources to investigations under the federal False Claims Act. Funds will be channeled to U.S. attorney's offices with a "proven track record" in such cases. She did not provide further details.

Covered entities that have already modified business associate contracts to comply with the HIPAA privacy rule may need to add additional language to comply with the security standards, notes attorney Reese Hirsch. Fortunately, providers have more than two years to make those additional changes

Final HIPAA Security Rule, *from p. 1*

In one important example, the proposed rule had called for chain-of-trust agreements to ensure that individually identifiable health information remains secure when it is transferred from a covered entity to a non-covered entity. The final rule eliminates the chain-of-trust reference, instead requiring that contracts with business associates contain assurances that such information will be safeguarded.

Reece Hirsch

"The U.S. Department of Health & Human Services has accomplished its goal of more consistency between the security rule and the privacy rule," says Reece Hirsch, a partner in the San Francisco office of Sonnenschein Nath & Rosenthal. "We can see this in a lot of ways, from the common defined terms to the elimination of the chain-of-trust agreement. There seems to be a much more flexible and scalable set of standards."

The final security rule requires covered entities to implement administrative, physical and technical safeguards for electronic protected health information in their care. Covered entities must comply with the security standards by Apr. 21, 2005. Small health plans will have an additional year.

As HHS notes in the final rule, security and privacy are inextricably linked. The privacy of information depends in large part on the existence of security measures to protect it. The security standards require covered entities to implement basic safeguards against unauthorized access, alteration, deletion and transmission.

The privacy rule, by contrast, sets standards for how protected health information should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to the health information maintained about them.

Streamlined & Narrowed

In general, HHS has streamlined the security rule, narrowing its scope to electronic information only and reducing the number of mandatory requirements—called implementation specifications—from 69 to 13, notes Hirsch. HHS also lists a number of "addressable" standards that give providers implementation options.

"With [those] standards, HHS places the burden back on the covered entity to make a determination of what's reasonable for them," he tells *GCR*. "All in all, the rule reflects a dose of reality and an understanding by the government that some of the requirements of the proposed rule were going to be very difficult for many sectors of the healthcare industry to implement."

As expected, HHS has also removed the standards for electronic signatures contained in the 1998 proposed security rule. The agency says it will publish these as a separate rule at a later date.

HIPAA Compliance Deadlines Ahead

2003

Apr. 14 Privacy – all covered entities except small health plans.
Apr. 16 Electronic Healthcare Transactions and Code Sets – all covered entities must have started software and systems testing.
Oct. 16 Electronic Health Care Transactions and Code Sets – all covered entities that filed a one-year extension request in 2002 and small health plans.

2004

Apr. 14 Privacy – small health plans.
July 30 Employer Identifier Standard – all covered entities except small health plans.

2005

Apr. 21 Security Standard – all covered entities except small health plans.

2006

Apr. 21 Security Standard – small health plans.

Source: HHS

Resources

- Final HIPAA security rule, online at *www.cms.hhs.gov/hipaa/hipaa2/default.asp*.
- Reece Hirsch: 415-882-5040

For the Record

A reader who works for a medical center that runs a 125-clinic laboratory outreach program wants to know who has ultimate responsibility for obtaining an Advance Beneficiary Notice (ABN) from a Medicare beneficiary.

Most of the clinics, the reader notes, collect blood specimens, then forward them to the lab with appropriate test requisitions and ABNs. But a few clinics next to the hospital send patients to the hospital's lab for the blood draw, and in some cases, the patients have not received an ABN.

"Our phlebotomist is not trained in local medical review policies, national coverage decisions or ABN delivery," writes the reader, who says the lab is under the impression that the physician is responsible for obtaining the ABN.

The short answer from the Centers for Medicare & Medicaid Services is that the laboratory performing the testing and submitting the related claim to Medicare has final responsibility for obtaining the ABN. The agency does, however, encourage doctors to obtain the ABN when they see the beneficiary.

CMS addresses the issue of lab responsibility in a series of frequently asked questions on its Website (*http://cms.hhs.gov/medlearn/refabn.asp*). Below are several of the relevant questions and the agency's answers:

Q: *A physician orders a lab test, and the lab does both the specimen collection and the lab test/processing. Is the lab or the physician responsible for executing the ABN?*

A: Because the laboratory has the risk of financial liability in case of a denial, it is the lab's responsibility to execute the ABN. The physician may execute the ABN, but this is not a requirement. If the physician has executed an ABN, the lab need not repeat it.

Q: *If a physician is "not responsible" for executing an ABN when a laboratory will bill Medicare for the test, why do you encourage the physician to execute an ABN in these situations?*

A: By "not responsible" we only mean that the physician is "not required by law" to execute an ABN for a test for which Medicare payment to the lab is likely to be denied. Nevertheless, a physician endeavoring to provide the best care to patients may wish to deliver an ABN. In this situation, the physician has immediate contact with the patient during the office visit or specimen collection, and is thus in the best position to have a meaningful dialogue with her/him regarding the choices to be made in going forward with the test or declining it. By delivering the ABN, the physician also is working in partnership with the laboratory that serves the practice (since the lab may not even encounter the patient), and this will help the lab remain financially solvent and available to the patients of the practice. While we do not mandate this partnering between physicians and their affiliated labs, we certainly encourage it. The best practice in this situation is for the patient to receive any necessary ABN at the physician's office.

Have a compliance question you'd like answered? E-mail it to Kimberly Scott, managing editor, at *kimscott@yahoo.com*.

OIG Suggests Lowering Outpatient Payments

Medicare could save as much as $1 billion annually by lowering reimbursement rates for some hospital outpatient procedures, HHS Inspector General Janet Rehnquist said Feb. 6 in remarks to the 6th Annual National Healthcare Compliance Congress, held in Washington, DC.

A new OIG audit of 453 outpatient procedure codes found that providers were reimbursed substantially more for 279 procedures when these were billed as rendered in hospital outpatient departments than when the same procedures were billed as rendered at ambulatory surgical centers (ASCs), she reported.

"In the absence of a compelling reason for a payment differential, the amount Medicare pays for a procedure code should be based on the service, not the setting."

Need to know all about the latest CLIA QC and HIPAA security, privacy directives? Join us at the G-2 Compliance & Policy Forum, Mar. 20-21, Tampa Westshore Marriott Hotel, Tampa, FL. To register or get more information, call 1-800-522-7347 or go to www.g2reports.com

More Cardiac Settlements: Five hospitals in Texas, Washington, Oregon and Florida will pay the Federal Government $4.9 million to settle allegations that they improperly billed Medicare for medical procedures involving experimental cardiac devices. Methodist Hospital and St. Luke's Hospital Episcopal in Houston agreed to pay $2.75 million and $575,000 respectively; Deaconess Medical Center in Spokane, $775,000; Legacy Good Samaritan Hospital and Medical Center in Portland, $410,000; and Orlando Regional Medical Center, $390,000. These latest settlements bring to $45+ million the total recovered in the nationwide false claims litigation involving such devices.

Prohibited Referral Charges Dismissed: The U.S. District Court for the Central District of Illinois has rejected a *qui tam* suit alleging that a hospital submitted false claims to federal healthcare programs without disclosing the existence of prohibited referrals. The court ruled that Constantino Perales, MD, failed to introduce evidence that purchases of medical practices by St. Margaret's Hospital (Spring Valley, IL) were above fair market value and thus he could not show any violation of either the anti-kickback law or the Stark physician self-referral statute.

Johns Hopkins Dinged On Teaching Physicians: Johns Hopkins University (Baltimore, MD) has agreed to pay $800,000 to resolve charges that it fraudulently billed Medicare for the services of certain faculty physician employees when the medical services were actually furnished by an intern or resident of the teaching hospital. But JHU does not have to enter into a corporate integrity agreement. To receive separate Part B payment, a teaching physician must personally provide a service or be present when a resident/intern furnished the care. This is the latest settlement in the HHS OIG's PATH initiative, which is scrutinizing compliance with Medicare payment rules for physicians at teaching hospitals.

Anti-Fraud Funding Leveling Off: Mandatory funding for Medicare fraud-fighting will level off in fiscal 2004 for the first time in seven years. Under the President's budget request for FY '04, the Centers for Medicare & Medicaid Services' Medicare Integrity Program, which funds claims audits and medical reviews, would get $720 million, the same as in FY '03. The HHS Office of Inspector General would get $160 million, with an expected decrease of 81 full-time equivalent positions. The money would come from the Health Care Fraud and Abuse Control Program established under HIPAA (the 1996 Health Insurance Portability & Accountability Act).

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.