CCH Healthcare Compliance LETTER

Volume 7, Issue 18 health.cch.com September 7, 2004

Identity theft case is first HIPAA conviction

by Suzanne Szymonik, JD, Contributing Editor

An employee of a Seattle cancer care center who obtained a cancer patient's name, date of birth, and Social Security number, and then used that information to get four credit cards and charge more than $9,000, pled guilty to wrongful disclosure of a patient's protected health information. This marks the first criminal conviction under the 1996 federal law that protects patients' privacy rights regarding medical information, the Health Insurance Portability and Accountability Act (HIPAA) (PubLNo 104-191).

HIPAA makes it illegal to disclose protected, individually identifiable health information to another person, for an impermissible purpose, knowingly and with intent to use the information for personal gain. Convicted defendants face imprisonment for up to ten years and fines up to $250,000.

The employee, Richard A. Gibson, signed a plea agreement on August 19, 2004, that contemplates a sentence of 10 to 16 months. He also agreed to make restitution to two credit card companies and to the cancer patient who incurred expenses fighting the identity theft. A prison term is expected because Mr. Gibson knew that the patient suffered from a rare and often fatal form of cancer, which made the patient a "vulnerable victim" according to federal sentencing guidelines. The court has not yet accepted the plea agreement. (*U.S. v. Gibson, W.D. Wash., No.CR04-0374 RSM*) ■

CCH Chicago Bureau, August 27, 2004

OCR clarifies Privacy Rule, state public records laws relationship

by Sharon Sofinski, Coordinating Editor

The Office for Civil Rights (OCR) recently posted a question and answer regarding the relationship of the HIPAA Privacy Rule to state public records laws. According to the Q&A, only states that are covered entities are subject to the HIPAA Privacy Rule. If a state public records law mandates that a covered entity disclose protected health information (PHI), the Privacy Rule permits the covered entity to make the disclosure, as long as the disclosure complies with the state public records law. However, if the state public records law only permits—and does not mandate—disclosure of PHI, or if exceptions or other qualifications exempt the PHI from the state law's disclosure requirement, the disclosures are not required and would not fall under the Privacy Rule. The complete Q&A is at: http://answers.hhs.gov/cgi-bin/hhs.cfg/php/enduser/std_alp.php. ■

CCH Chicago Bureau, August 31, 2004

Letters to the Editor

The CCH Healthcare Compliance team welcomes comments or questions regarding articles published in the CCH Healthcare Compliance Letter. Send comments to Sharon Sofinski, Coordinating Editor, at sofinsks@cch.com. For more information about the CCH Healthcare Compliance Portfolio visit our online store at http://health.cch.com.

Long-run goal of compliance should be improving performance, expert says

by Catherine Hubbard, MA, Contributing Editor

An effective compliance program should yield a lower claims rejection and error rate, but more importantly, it should establish within an organization the structure and culture of best business practices, according to John Beattie, director of healthcare operational and compliance services at Parente Randolph, Harrisburg, Pennsylvania. "Culture is very essential. Ethics must be a driving force of the enterprise," he said during a Health Care Compliance Association audioconference on compliance effectiveness held on August 12.

While the government currently focuses on correct billing fostered through auditing and monitoring programs, education and training, and corrective action, Beattie said, the long-run goal of an organization should be creating a culture of compliance and improving performance. "Billing is not going to be in the long run the sole measure of the effectiveness of a compliance program," he predicted.

One of the true measures of effectiveness is an awareness of and focus on building an integrity-centered organization, Beattie said. "Hospitals are very complex organizations with constantly changing rules and interpretations. It's what we do not know and how long it takes us to discover what we do not know that may over time become the true measure of an effective compliance program," he predicted.

Also at the audioconference, Stephan Vincze, vice president of ethics and compliance and privacy officer for TAP Pharmaceuticals, Chicago, Illinois, stressed that by working with others at the organization and with the government, compliance officers will produce positive results. He encouraged people to get past the "us against them" perception and foster a partnership.

Beattie added that partnership principles are particularly important for compliance officers, which he called "a catalyst for change and for performance improvement." He stressed that compliance officers should work closely with employees in the organization. "You cannot bury yourself," he said. "You have to get up and walk around the institution." He added that "Documentation is not going to tell you the whole story," recommending compliance officers talk with people about the policies and procedures and ask what really goes on in the organization. "You need to have a rapport with the employees of the organization in order to get honest answers. You cannot lead if you're distrusted," he said.

"What could be deemed an effective compliance program today may not be so at a later time."

Shawn DeGroot, vice president of corporate compliance, Rapid City Regional Hospital, Rapid City, South Dakota, said that when meeting with and speaking to employees, compliance officers should be aware of facial expressions, posture and hand gestures. Some hand gestures, such as open palms, can help foster learning and compliance, while other gestures, such as hands behind the head, a sign of arrogance, will distance the speaker from others, she said.

Employee training. Vincze suggested compliance officers take a multi-dimensional approach toward training. "You should not rely on any one meaning of training," he said. He recommended a mixture of computer-based training that includes true to life scenarios and interactive features, and live training where the company can customize seminars with each functional area of the organization, such as human resources, finance, sales and marketing.

During live sessions, Vincze said, instructors should present some case studies and encourage the class to discuss the code of conduct issues involved and how those issues apply to the facts of the case. "Keep it simple," he urged, stressing that the presenter should focus on one or two key points.

One relatively low-cost method of training and education is to hold an audioconference, during which people can tap in to the program and ask questions, Vincze said, adding that these meetings are especially useful, since they allow for live interaction. "The more people feel comfortable coming to you as a resource to ask questions, the more likely you'll be seen as an added-value partner in your organization," he said.

CCH Healthcare Compliance LETTER

Managing Editor
Pamela K. Carron, J.D.

Coordinating Editors
Angela Fanelli, J.D.
Sharon Sofinski

CCH Washington Bureau
Paula Cruickshank
DOJ, FTC–John Scorza
SEC–Peter Feltman
Health Law–Catherine Hubbard
Tax–Jeff Carlson, David Hansen

Designer
Jason Wommack

Comments from readers are welcome and should be directed to Sharon Sofinski at SOFINSKS@CCH.COM, Tel. 847-267-7860, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Healthcare Compliance Letter is published 24 times a year by CCH INCORPORATED, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is $305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Healthcare Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

Antitrust

Physician-hospital organization settles FTC price fixing case

by CCH Editorial Staff

A North Carolina physician-hospital organization (PHO) and ten of its physician members would be banned from collectively negotiating with payors on behalf of physicians and setting the prices or other terms on which physicians deal with payors, under the terms of a proposed FTC consent order. The proposed order would also prevent the PHO, for a period of time, from operating as a "messenger," or contracting agent, on behalf of physicians in dealing with payors. The proposed consent order would settle FTC charges that the PHO and its members fixed prices for the services of the PHO's 450 physician members, hindered competition in four western North Carolina counties, and raised costs for consumers. The proposed order would allow the PHO to engage in potentially procompetitive activities, such as information technology and medical management services, that do not pose a significant risk of anticompetitive effects.

The FTC issued its administrative complaint late last year against the PHO and the ten members. At that time, an acute care hospital in Hickory, North Carolina, and its parent company settled FTC charges concerning their role in the allegedly unlawful activities. ■

CCH Chicago Bureau, August 18, 2004

Best Practices (cont.)

Continued from page 2

During any presentation, a compliance officer must be credible, yet not too authoritative or grave, Vincze said. He advised officers to make the meetings fun by adding some jokes and by providing positive competition and incentives to encourage compliance. "You can have some fun with it," he said.

"We should have fun when we do compliance," Beattie added.

Yet compliance programs also must be taken seriously, Beattie said. "You could have all the policies and procedures in place, but if management winks at these or if a nursing staff or patient care employee views these policies as sanctimonious hypocrisy by management, the number of policies and procedures only serve to further indict your program," he warned.

Measuring effectiveness. Vincze said compliance officers should establish concrete goals. "Shift your focus from effectiveness to performance measurement, from criminal sentencing to good business practices, from abstract or vague concepts to practical and concrete tools and from more narrative discussion of effectiveness to more actual measurement of metrics," Vincze urged.

"The more we can measure empirically our success, [and] the more we can show compliance helps with efficiency, the more likely it will be accepted and seen as effective," added Beattie.

Beattie also noted that internal controls must be adjusted over time, particularly when there's a change in management, when there's a failure of internal controls, when there's routine processing without thinking or when there's a lack of information to make informed decisions. "What could be deemed an effective compliance program today may not be so at a later time," he said. ■

CCH Washington Bureau, August 27, 2004

On The Front Lines

Ready or not, here come the Security Rules

by Harris Beach, LLP

The jury is still out regarding whether the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the federal legislation that seeks to make fundamental changes in the health care industry, will have the result that was envisioned. It certainly has, however, already made a large impact on operations of entities that deal with health care data and information–and in April 2005, the impact will become even larger.

Background

HIPAA was implemented, according to its legislative history, to improve the current domestic health care system, which has experienced heavy regulation, double-digit inflation, and lawsuits. The statute's three goals are: (1) to promote portability of health insurance among employers; (2) to greatly expand the statutory weapons available to prosecute health care fraud; and (3) through "administrative simplification," to promote uniformity and confidentiality in the use and transmission of health information.

It is under this third goal that the Privacy and Security Rules of HIPAA fall. The "Security Rules" are the final federal security standards for health care information, issued on February 13, 2003. When releasing the Security Rules, the Department of Health and Human Services (HHS) pointed out that "certain health care providers and health care clearinghouses must establish procedures and mechanisms to protect the confidentiality, integrity and availability of electronic protected health information." How to implement such protections is at the forefront of all covered entities as the April 2005 compliance deadline looms. The rules require all covered entities to implement administrative, physical, and technical safeguards to protect electronic protected health information (EPHI) in their care.

This was not the first time security issues were addressed. In the preliminary Security Rules, released in 1998, a single sentence mentioned the need for chain-of-trust agreements to ensure personal health information remains secure when it is transferred from a covered entity to a non-covered entity. Thus, for example, the health care plan's transmission of data to a third-party administrator would be a "chain-of-trust" that would require protection of the data. The final HIPAA Privacy Rules include a requirement of business associate agreements for the same purpose, but for all intents and purposes eliminate the strict notion of protecting every link in the chain.

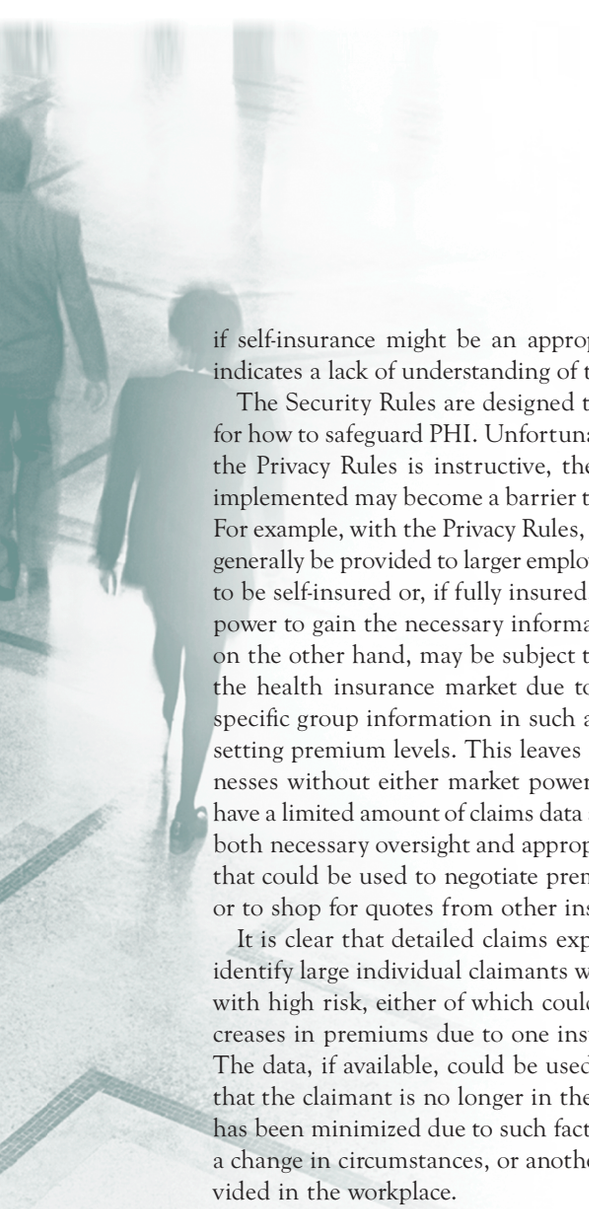
It is significant to note that HHS actually narrowed the scope of the Security Rules to better align with the Privacy Rules. Under the proposed Security Rules, the scope was originally health information that related to an individual and that was electronically maintained. Under the final rules, however, if data is de-identified as not being secure, it is not covered under the Security Rules. Also, in releasing the Security Rules, HHS removed the electronic signature requirement; it was then subsequently included in a separate regulation.

In the final Security Rules, health care plans must understand the distinction between "addressable" and required implementation specifications. Addressable specifications are not mandatory, thus allowing variable levels of compliance from entity to entity. The number of mandatory implementation specifications decreased from 69 in the preliminary rules to 13 in the final rules.

Furthermore, the Security Rules make no distinction between internal and external data movement, with security procedures required of both. Simply put, the Security Rules cover EPHI in storage as well as during transmission. Fortunately, HHS recognized in the Security Rules that each entity's security needs are unique, and, therefore, the specific protections deemed appropriate to adequately protect information will vary and will be determined by each entity in complying with the standards. This is especially critical for health care plans, as data may move internally for purposes or preparing such documents as Form 5500, the reporting vehicle for health care plans under the Employee Retirement Income Security Act (ERISA).

Practical Aspects

There is an inherent danger in the confusion generated by the Security Rules. The tighter standards imposed on business relationships and the sharing of data among a health insurer and a health plan, the plan sponsor, and insurance brokers have created confusion and, in some aspects, paranoia. There are popular press reports that in many cases, insurers are denying specific claims information to fully insured employers who agree to certain safeguards, which insurance brokers, employers, and some attorneys complain is an overly cautious approach that will ultimately stifle competition and further escalate health costs. The lack of health care data is limiting the ability of health care plans to negotiate more favorable premium rates, or to make the necessary analysis to determine



if self-insurance might be an appropriate alternative. This indicates a lack of understanding of the Security Rules.

The Security Rules are designed to provide a framework for how to safeguard PHI. Unfortunately, if experience with the Privacy Rules is instructive, the standards when fully implemented may become a barrier to relevant information. For example, with the Privacy Rules, claims information can generally be provided to larger employers who are more likely to be self-insured or, if fully insured, have sufficient market power to gain the necessary information. Small employers, on the other hand, may be subject to community rating in the health insurance market due to state protective laws; specific group information in such a case is not relevant in setting premium levels. This leaves a large number of businesses without either market power or legal protection to have a limited amount of claims data available, thus reducing both necessary oversight and appropriate and accurate data that could be used to negotiate premiums with the insurer or to shop for quotes from other insurers.

It is clear that detailed claims experience is necessary to identify large individual claimants within a group, or those with high risk, either of which could result in dramatic increases in premiums due to one insured who is an outlier. The data, if available, could be used to show, for example, that the claimant is no longer in the group or that the risk has been minimized due to such factors as new medication, a change in circumstances, or another accommodation provided in the workplace.

Overview of the Security Rules

The following is a brief overview of the Security Rules, intended to provide a general understanding of the most significant provisions. This overview is not intended to address all of the issues, nor does it offer a step-by-step "how to" for compliance. Rather, it is simply a framework for understanding the Security Rules, which will assist in understanding the upcoming compliance efforts.

The Security Rules begin with a requirement, from both a legal and practical viewpoint, that a risk analysis be conducted. Specifically, the Security Rules require employers to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." Furthermore, the Security Rules direct affected employers to understand that "[t]he required risk analysis is also a tool to allow flexibility for entities in meeting the requirements of this final rule. . . ."

The Security Rules emphasize that risk assessments are to be ongoing, conducted frequently yet with minimal disruption to operations. Simply put, when the risk to an organization changes—for example, when there are changes in organization's operations and environment—a new risk assessment should be conducted. Accordingly, organizations must establish a risk assessment program and methodology that includes a regular review and immediate identification of risks. The program must include follow-up risk assessments to ensure that changes to the organization are identified along with any changes in the risk profile of the organization. Of course, changes to software and/or hardware programs must be analyzed and assessed before final implementation to assess whether there have been changes to the risk profile, thus requiring security features.

Covered Entity

It is critical to understand when an entity will be subject to the Security Rules. As with the Privacy Rules, the Security Rules are applicable to all covered entities with respect to PHI.

A covered entity is any health plan, health care clearinghouse, or health care provider that transmits any health information in electronic form in connection with a standard transaction. The Security Rules have a special application to two additional types of entities: affiliated covered entities (ACE), and hybrid entities. Legally separate covered entities that are under common ownership or control may elect to be treated as ACEs for purposes of compliance with the Security Rules.

In addition to the ACE, the Security Rules have special application to hybrid entities and covered entities with multiple covered functions. A hybrid entity is a covered entity that performs both covered and non-covered functions and whose covered functions are not its primary functions. The hybrid entity must designate and document which component or components of its business would, if performed by a separate legal entity, make that entity a covered entity. Only those portions of the hybrid entity's business that coincide with a covered entity's function would be subject to the Security Rules. The hybrid covered entity is obligated to ensure that employees who perform functions for both the covered and uncovered portions of the hybrid entity do not use or disclose PHI obtained while providing services to the covered portion of the hybrid entity in a manner that is inconsistent with the Security Rules.

Protected Health Information

PHI is defined as "individually identifiable health information" that is transmitted in electronic media, maintained in an electronic medium, or transmitted in any other form or medium. PHI, however, does not include certain educational records covered by the Family Educational Right and Privacy Act and certain other education-related documents. In order to eliminate confusion and ease implementation, the Security

Rules were written to complement the Privacy Rules. The Security Rules do not specifically address privacy but were drafted to protect electronic protected health information (EPHI) from unauthorized access or modification. They define administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of EPHI.

The Security Rules require covered entities to implement basic safeguards to protect EPHI from unauthorized access, alteration, deletion, and transmission. The Privacy Rules are different in that they set standards for how PHI should be controlled by defining the uses and disclosures that are authorized or required, and patients' rights with respect to their health information.

The Security Rules require protection of such information, but they only cover information that is in electronic form. Standards for the security of all health information or PHI in nonelectronic form may be proposed at a later date. Certain information, from which identifiers have been stripped, is not covered by the Security Rules.

Addressable Versus Mandatory Requirements

As noted above, HHS adopted both required and addressable implementation specifications when releasing the final Security Rules. By way of background, HHS, in deciding what entities would have to accomplish in order to be compliant with HIPAA, set forth three principles:

- The standards should be comprehensive and coordinated to address all aspects of security;
- The standards should be scalable so they can be effectively implemented by covered entities of all types and sizes; and
- The standards should not be linked to specific technologies, allowing covered entities to make use of future technology advancements.

In the comment period following the release of the proposed security rules, HHS received many comments that the large number of required security standard implementations (69, to be exact) was too burdensome to be considered reasonable. Employers especially were concerned that compliance with the Security Rules would become something akin to a separate line of business, requiring many dedicated workers and full-time compliance efforts.

In response, HHS introduced the concept of addressable, or optional, implementation specifications to allow covered entities additional flexibility in complying with the Security Rules. The final Rules allow each covered entity to choose, based upon its own risk assessment, which of the addressable standards should be met. According to HHS, when dealing with an addressable standard, each covered entity has the option to:

- Implement one or more of the addressable implementation specifications;
- Implement one or more alternative security measures;
- Implement a combination of both; or
- Implement neither an addressable implementation specification nor an alternative security measure.

The decision to implement addressable specifications may be made, according to HHS, based upon a number of factors, including but not limited to:

- The entity's risk analysis;
- The entity's risk mitigation strategy;
- Consideration of the security measures already in place; and/or
- The cost of implementation.

In its discussion of whether cost should be a primary factor, HHS specifically noted that cost may be used as a major or the sole factor in determining the scope of implementation of an addressable specification. Thus, implementation of the addressable specifications may boil down to a business decision.

A covered entity must take the following into account when making its decision:

- If a given addressable implementation specification is determined to be reasonable and appropriate, the covered entity must implement it. This is a difficult standard for a covered entity, as "reasonable and appropriate" could be considered in the eye of the entity. With health care inflation so rampant, any additional cost might not be considered "reasonable and appropriate" as it adds to the already unreasonable burden placed upon the plan sponsor and participant. A different, more appropriate determination is whether the "reasonable and appropriate" standard is met in the context of not only health care costs, but also in the spirit of compliance with the Security Rules.
- If a given addressable implementation specification is determined to be an inappropriate and/or unreasonable security measure for the covered entity, but the standard cannot be met without implementation of an additional security safeguard, the covered entity may implement an alternate measure that accomplishes the same end as the addressable implementation specification. Covered entities may not be fully familiar with alternatives initially, but consultants and experience will certainly give rise to alternate measures.

Standards

In all cases, the covered entity must meet the standards set forth in the Security Rules. Covered entities must implement the required specifications; cutting back on the required specifications to save money or because the compliance officer believes the requirement is not necessary is simply not allowed. The final standards, however, are reasonable in light of what could have been required, and after initial compliance, employers will likely not feel a considerable negative impact. In fact, many employers may already have implemented standards that comply with the Security Rules, and simply have to document their existence in a more formal process.

Enforcement

All the experts agree that HIPAA enforcement—or the threat of it—is what will drive compliance. It is not enough to simply set forth a monetary penalty for violating

HIPAA; there must be evidence of enforcement to encourage entities to comply.

To that end, legislation authorizes the Secretary of HHS to impose civil monetary penalties, in an amount of not more than $100 per violation, not to exceed $25,000 for all violations of the same provision in a calendar year, on any covered entity that violates any of the HIPAA provisions, including the Security Rules. There are also a number of procedural requirements for the imposition of civil monetary penalties.

A caveat must be included with this discussion. The enforcement rules will not become relevant to covered entities unless there has been an alleged violation. Nevertheless, attorneys will find these rules important. Since the rules are highly technical in nature, entities should always enlist counsel for assistance when dealing with enforcement proceedings.

Framework for Penalties

To provide a procedural framework for levying civil monetary penalties, on April 17, 2003, HHS published its interim final rule governing the investigation, adjudication, and imposition of civil monetary penalties for violations of any of the HIPAA provisions (the "Interim Rule"). Entitled "Civil Monetary Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings," the Interim Rule is the first installment of the HIPAA "Enforcement Rule." When issued in final form, the Enforcement Rule will outline comprehensive procedural and substantive requirements relating to the imposition of civil monetary penalties on any covered entity that violates the HIPAA Administrative Simplification provisions.

Many believe that the enforcement Interim Rule relates only to Privacy. That is only true for a short while longer, as the Security Rules are not yet enforceable; however, it is advisable to read the Interim Rule in the context of the Security Rules and comment accordingly, as the same framework enunciated in the Interim Rule will eventually be applicable.

The Interim Rule contains the first iteration of the procedural framework for enforcement. The provisions of the Interim Rule became effective on May 19, 2003, and expire on September 16, 2004. Although the procedural rules contained in the Interim Rule are technically exempted from the notice-and-comment rulemaking procedures, HHS allowed comments on the Interim Rule through June 16, 2003, and may revise certain of the procedures contained in the Interim Rule by its September 16, 2004 expiration date.

HHS's General Approach to Enforcement

In publishing the Interim Rule, HHS reiterated its intent to seek voluntary compliance with the HIPAA provisions. Consistent with the requirements of HIPAA, HHS, through the Office of Civil Rights (OCR) and the Centers for Medicare and Medicaid Services (CMS), intends to seek cooperation of covered entities with meeting the HIPAA requirements to the extent practicable, and has the authority to provide technical assistance to help covered entities come into voluntary compliance. Enforcement will primarily be a complaint-driven process, and will include progressive steps that provide a covered entity with an opportunity to demonstrate compliance or to submit a corrective action plan.

Knowing that voluntary compliance is a goal and not a reality, HHS has taken a number of steps. First, it has stated that it intends to assist covered entities with compliance. At the same time, effective May 19, 2003, HHS has established a procedure by which civil monetary penalties may be imposed in the event they become a necessary enforcement tool.

Provisions of the Interim Rule

The provisions contained in the Interim Rule may be broken down into three subsections: (1) the investigation provisions, (2) the civil monetary penalty provisions, and (3) the administrative hearing provisions. Taken together, these three subsections lay a foundation for the imposition of civil monetary penalties based upon a violation of the HIPAA provisions.

These are the technical portions of the rules that will be of more interest counsel rather than the covered entity. Some issues may come to the attention of the covered entity immediately, for example, in the event it is served with an investigational subpoena. It cannot be stressed enough that counsel should be immediately enlisted for assistance. At the same time, compliance is always an appropriate starting point in order to answer the questions "why should we" or "what if we don't?"

Conclusion

With only two full quarters left before implementation date, covered entities must begin their Security Rules compliance effort immediately. Those that have already begun compliance efforts already know full well that this is an effort not to be taken lightly ... or too late. ■

Harris Beach, LLP, is a top 250 law firm with offices throughout the Northeast. Since its founding in 1856, it has provided wide range of legal services for a broad-based clientele. Harris Beach's Health Services Department has been at the forefront of structural changes in the rapidly evolving health care industry. Harris Beach attorneys counsel a wide variety of institutional and individual health care providers, multi-provider organizations, managed care organizations and insurers, and have substantial experience in integrated delivery systems and managed care products. Harris Beach's health services include mergers, acquisitions, affiliations, and reorganizations; general corporate; antitrust; regulatory compliance; operations' medical malpractice defense and risk management advice; labor and employment issues; third party reimbursement; financing services; tax, pensions, and employee benefits; and real estate and environmental issues. They regularly provide compliance advice regarding the privacy and security provisions of Health Insurance Portability and Accountability Act of 1996 (HIPAA) to a wide range of clients, including skilled nursing facilities, physician groups, large corporations and free-standing surgical centers. Their attorneys prepare consents and authorizations, modify business associate contracts and agreements, and perform structural and organizational evaluations for organized health care operations to achieve and maintain HIPAA compliance.

Harris Beach authored the CCH HIPAA Privacy Guide, CCH HIPAA Security Guide, and CCH HIPAA Guide for Employers. For information on ordering these Guides, call 1-800-449-9525.

GAO, OIG evaluate fraud oversight

by Michelle L. Oxman, JD, Contributing Editor

CMS's oversight of states' Medicaid fraud control units does not examine the effectiveness of these programs, and its allocation of resources to oversight "may be disproportionately small" in light of the risks, according to a recent Government Accountability Office (GAO) report. The GAO report was published on the heels of an annual report issued by the Office of Inspector General (OIG) lauding the efforts of state Medicaid Fraud Control Units (MFCUs). Collectively, state MFCUs claimed total recoveries of more than $268 million in fiscal year 2003 from court-ordered restitutions, fines, settlements, and penalties. A total of 1,096 convictions were also obtained in that period.

Fraudulent billing and upcoding common. Both agencies surveyed U.S. states and territories about their fraud control and program integrity efforts. Forty-seven states completed the GAO's inventory. The OIG's report covered the participants in its MFCU grant program, which included 47 states and the District of Columbia. The OIG's report describes various state efforts to combat fraud and abuse, concentrating on anecdotal reports of success but not naming perpetrators of fraud. The OIG included but did not discuss a table that shows that 21 states did not recoup the amount of their fraud-control grants in fiscal 2003.

Both reports discussed the most common forms of Medicaid fraud and abuse. Providers of all types billed for services that were never provided and upcoded to more expensive procedures. Some medical centers and nursing homes billed the government for services performed by unlicensed or unqualified staff as if they had been performed properly. One laboratory provided free enteral feeding pumps as marketing incentives to providers and suppliers and advised them to bill both Medicare and Medicaid for the equipment.

Enrollment controls, new technology effective. The GAO found that states that reported enrollment controls such as on-site inspections, criminal background checks and time-limited enrollment reduced improper payments. Cancellation or suspension of inactive provider billing numbers prevented fraudulent use of those numbers. The GAO also found that requiring a surety bond helped reduce financial loss. Some states used these techniques with all providers and suppliers; others used them only with those considered high risk.

"Providers of all types billed for services that were never provided and upcoded to more expensive procedures."

Many states used new technology to scrutinize claims for patterns of suspicious behavior. The use of formularies and menu-driven pre-authorization systems helped to prevent abusive prescription practices. Integrated databases of providers, claims and beneficiaries revealed that some practitioners billed twice for the same services or billed for more services than were possible in one day. Mining data for utilization patterns and comparing providers within specialties helped officials distinguish between typical and aberrant patterns. CMS's pilot program combining Medicare and Medicaid databases was estimated to have achieved a 21 to 1 return on investment in its first year in California, about $58 million in recouped overpayments, costs avoided and savings.

Other CMS Practices. CMS's primary means of oversight of state program integrity work is on-site compliance reviews. The GAO found that because of resource limitations, CMS had reviewed only 29 state programs between 2000 and 2003 and planned to review about 8 states per year in the future. CMS had allocated eight full-time staff and $26,000 for expenses for the 2004 national oversight effort, a decrease from $80,000 in fiscal 2002. The current level of spending allows CMS to review each state's activities every six years. With federal Medicaid expenditures of $139 billion in 2002, there is a great risk of serious financial loss and the current level of oversight is insufficient, according to the GAO.

Although CMS claimed that its increased financial management staff will better address fraud in state programs, the GAO concluded that this response is inadequate. In February 2002, the GAO reported that CMS's on-site reviews did not evaluate the effectiveness of state fraud and abuse programs. According to the GAO report, there has been no change.

State MFCU performance is evaluated by the OIG against twelve set standards. Units must: (1) conform to all applicable statutes and regulations; (2) employ sufficient professional staff, including attorneys, auditors, and investigators; (3) establish policies and procedures; (4) maintain adequate workloads; (5) cover all provider types in case mixes; (6) close cases in reasonable time periods; (7) monitor case outcomes; (8) cooperate with federal fraud authorities; (9) make recommendations to state government; (10) review memoranda of understanding with state Medicaid agencies; (11) exercise proper control over resources; and (12) maintain training plans. ■

CCH Chicago Bureau, August 27, 2004