CCH Health Care Compliance LETTER

Volume 8, Issue 11 health.cch.com May 25, 2005

CMS posts FAQs on HIPAA Security Rule

by Sheila Lynch-Afryl, JD, Contributing Editor

CMS, which is in charge of enforcing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, posted five new frequently asked questions (FAQs) to its web site concerning security incidents, risk analysis, and user IDs.

Security incident. A covered entity must implement policies to address, identify, and respond to suspected or known security incidents, which include the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

In order to maintain a flexible and technologically neutral approach to the Security Rule, no single method has been identified for addressing security incidents that will apply to all covered entities. In addressing the security incident procedures standard, however, a covered entity may consider some of the following questions:

- what specific actions would be considered security incidents;
- how will incidents be documented and reported;
- what information should be contained in the documentation;
- how often and to whom should incidents be reported;
- what are the appropriate responses to certain incidents; and
- whether identifying patterns of attempted security incidents is reasonable and appropriate.

Business associate reporting of security incidents. Even though a business associate may not be a HIPAA covered entity subject to the HIPAA Security Rule, its business associate contract may still obligate the associate to report security incidents to the covered entity. The covered entity and business associate must document the specifics of the reporting requirements in the contract, including the frequency, level of detail, format and other relevant considerations (e.g., in aggregate or per incident, weekly or monthly).

Reporting security incidents to a group health plan. Similarly, although a plan sponsor may not be a HIPAA covered entity, it would nevertheless be required, through its plan documents, to report security incidents to the group health plan. The plan documents could serve as the vehicle to establish a group health plan's specific reporting requirements and should be developed to meet the group health plan's specific needs.

Risk analysis. The risk analysis process identifies potential security risks to electronic protected health information (EPHI). The National Institute for Stan-

Letters to the Editor

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

dards and Technology, which provides information security guidance materials for federal agencies, categorized threats into three common categories: human, natural, and environmental. An example of a natural threat is the occurrence of an avalanche. An organization must assess the likelihood that a given threat will occur and develop a strategy to manage the threat.

User IDs. The Security Rule prohibits a covered entity from assigning the same log-on ID or user ID to multiple employees. Under the HIPAA Security Rule, covered entities, regardless of their size, are required to assign a unique name and/or number for identifying and tracking user identity. A "user" is defined as a "person or entity with authorized access." Accordingly, the Security Rule requires covered entities to assign a unique name and/or number to each employee or workforce member who uses a system that maintains EPHI so that the entity can identify and track which users are accessing the system. ■

CCH Chicago Bureau, May 5, 2005

Practical implications of HIPAA Security Rule

by Catherine Hubbard, MA, Contributing Editor

Health care organizations should conduct a thorough risk analysis of computer systems and physical settings to assure patients' electronic protected health information (EPHI) is secure and in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, according to Patricia Markus, a partner in Smith Moore's Raleigh, N.C. office. During a recent audio conference sponsored by the American Health Information Management Association (AHIMA), she suggested that organizations rank and prioritize threats based on two factors: (1) previous security incidents and (2) potential security incidents.

"Reduce risks and vulnerabilities to a reasonable and appropriate level with safeguards and fixes that prevent, deter, contain, detect and offset risks," Markus suggested. One way to reduce risk is to eliminate electronic transmission in non-critical areas, she added.

Risk management is an ongoing process that requires periodic monitoring, she stressed. Periodic reviews should include new hardware or software, a new service provided, or a new wing added to the health care organization.

Health care organizations should also have a regular auditing and monitoring system in place. A reporting system for violations that allows employees to report suspicious conduct anonymously should be implemented. "It is important to have a system in place so that when someone sees conduct that is suspicious, they know who to report it to and can do it anonymously without retaliation," she said.

Educating employees. Markus recommended training personnel in the health care organization as to basic security measures, such as establishing secure log-ins and passwords to develop a culture in which EPHI is protected. Managers and boards should act as role models, she emphasized. "They also need to be accountable," she said. Health care organizations should protect EPHI from improper modification or destruction, said Marcus. These organizations should also implement a system to verify the identities of people and entities seeking access to EPHI, with a focus on preventing the transmission of EPHI via the Internet.

Scalability. All covered entities must comply with the rule, but safeguards may vary, Markus said, noting that the rule is technology neutral. "You do not have to implement specific security technology," Markus explained.

Moreover, the Security Rule is intended to be scalable. "The safeguards you implement will vary depending on the size of your organization and the amount of personnel and resources," she said. She added that a program needs to protect the security of both EPHI and PHI that is on paper.

Backup plan. Health care organizations should take preventative safeguards and fixes including establishing firewalls, controlling modems, backing up data and establishing a system for recovering data in an emergency. To deter, detect and offset risks, health care organizations should establish policies and procedures, train employees, create audit trails, form a contingency plan and purchase insurance.

The main security risks are loss or corruption of EPHI due to a disaster or a hacker, temporary loss or unavailability of records due to a system crash or power outage, unauthorized access to or

CCH Health Care 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, Steve Cooper

Designer
Laila Gaidulis

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 Health Care 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 Health Care Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

disclosure of EPHI and loss of physical assets, said Markus. "Have systems in place so that you can continue to operate," she suggested. ■

CCH Washington D.C. Bureau, May 5, 2005

Enforcing HIPAA administrative simplification

by Catherine Hubbard, MA, Contributing Editor

Even though the new HIPAA Enforcement Rule is not final, it is not too soon to prepare by becoming familiar with some important changes, many of which expand the rule's scope.

In fact, the proposed new rule refers to procedural inadequacies and quirks that may be useful to know when arguing matters heard under the old rule, said Marc Goldstone, a partner with Hoagland, Longo, Moran, Dunst and Doukas, New Brunswick, N.J. during a May 6 American Health Lawyers Association audio conference.

Still, the old HIPAA Enforcement Rule, which sunsets in September 2005, is the one to follow, Goldstone emphasized. "The new rule is not a new rule yet," he said. "Until the new rule is published for final adoption, the old rule is still good law," he said. Comments on the proposed new rule are due June 17, he noted.

One of the key changes is that the proposed rule would broaden the definition of "persons" subject to the enforcement rule to include those defined as "a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private," Goldstone said. The interim final rule, in contrast, defined a "person" as "a natural or legal person."

Goldstone highlighted several other changes to expect. For instance, the proposed rule states that a violation occurs when a covered entity fails to take an action required by a HIPAA rule as well as when a covered entity takes an action prohibited by a HIPAA rule. Likewise, voluntary compliance enforcement, originally applicable only to privacy rules, is not proposed to apply to all HIPAA rules, he said.

In addition, under the new proposed rule:

- Administrative simplification is defined as any requirement or prohibition established by the HIPAA provisions or rules. "They can now enforce penalties against almost anything that is found in the rule," including technical violations and substantive violations, both material and immaterial, Goldstone said.
- HHS may use testimony and other evidence obtained in an investigational inquiry in any of its activities, yet PHI may be disclosed only if necessary. In addition, the secretary is required to impose civil monetary penalties if he or she discovers a violation of a rule.
- The new rule clarifies transcript procedures and states that a witness's right to retain a copy of the transcript of his or her testimony may be limited for good cause. If access is limited, then the witness may inspect the transcript and propose corrections. "If the record is incorrect, it is important to be able to get it corrected," Goldstone emphasized.
- Penalties would be public. When a penalty proposed by the secretary becomes final, the secretary notifies certain state and local agencies, plus the public. "I personally am uncomfortable with that," said Goldstone. "Once it is published, it's out there," he said. There are no standards concerning the content of the notice, its distribution, or the length of time a notice may remain in the public domain. Seeing that a penalty was issued without contextual material may convey an image to the public that the entity has serious privacy or security issues, when the problem may have been with a single "bad actor" employee, and the problem has been cured.
- A respondent would bear the burden of proof with respect to any affirmative defense or any challenge to a proposed penalty.
- There would be no mandatory fee cap on the respondent's attorney's fees.

In addition, Goldstone said he is concerned that rules of evidence in the enforcement process under this proposal are not harmonious with state court rules, adding that respondents may have to limit their case presentations at HHS as a tool to control their risk of state-court liability. "This may adversely affect their ability to defend the Federal charges," he said.

continued on page 7

Working without a net: Ethical considerations for in-house counsel in the investigation process

By William W. Horton

In the aftermath of the corporate crises that began with the collapse of the Enron Corporation and led to the adoption of the Sarbanes-Oxley Act of 2002,[1] there is a new spotlight on the role of in-house and outside lawyers. This spotlight is focused on the roles of such lawyers not only in the corporate response to those crises but also in the events that led up to them, and has resulted in both sharp criticism and potential civil and criminal liability for lawyers.

In the highly complex regulatory and business environment in which health-care enterprises operate, where there are often significant tensions between legal requirements and business strategies and where the penalties for crossing sometimes murky lines may be enormous, this new scrutiny poses new challenges for in-house counsel, as well as creating new dynamics for the interaction between inside counsel and outside counsel. This article will provide a brief overview of some legal and ethical issues for in-house counsel that arise when their clients come under investigation.

I. Evolving Legal and Ethical Responsibilities of Counsel with "Bad Information"

In each new corporate scandal, questions have been raised concerning the role of lawyers in the underlying events and on (i) how lawyers fulfill their duties to their organizational clients and (ii) what, if any, duties lawyers have to non-clients, including investors, regulators and the general public. These questions are, perhaps, most pointed in the in-house setting, where the in-house counsel's scope of organizational knowledge may make it more likely that counsel will become aware of potential wrongdoing, where those potentially involved may be close co-workers and "internal clients," and where the lawyer's own actions may invite intense personal scrutiny. In-house counsel must understand, before the crisis emerges, what legal and ethical responsibilities they have in investigating and responding to potential charges of organizational wrongdoing.

A. Rights and Responsibilities under the Model Rules

In August 2003, the American Bar Association adopted significant amendments to Rules 1.6 and 1.13 of the Model Rules of Professional Conduct.[2] As amended, Model Rule 1.6- the general rule governing confidentiality of information relating to the representation of a client- provides for the first time that an attorney may reveal client confidences without the client's consent (i) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and (ii) to prevent, mitigate or rectify such an injury resulting from a client's crime or fraud.[3] These amendments are permissive in nature, and only apply when the client has used or is using the attorney's services in furtherance of the crime or fraud.

Model Rule 1.13 is the general rule relating to the representation of organizational clients. Under the amended rule, where an attorney representing an organization knows that an employee or agent of the organization is acting, intends to act or refuses to act in a matter related to the representation that is (i) a violation of a legal obligation to the organization, or a violation of law that reasonably might be imputed to the organization, and (ii) likely to result in substantial injury to the organization, then the lawyer must proceed as is reasonably necessary in the best interest of the organization. Unless the lawyer reasonably believes that it is not necessary, the lawyer must refer the matter to "higher authority in the organization," including, if necessary, "to the highest authority that can act on behalf of the organization as determined by applicable law.[4]"

B. Rights and Responsibilities under the SEC "Attorney Conduct" Rules

In January 2003, the Securities and Exchange Commission (SEC) issued rules under Section 307 of the Sarbanes-Oxley Act[6] establishing minimum standards of professional conduct

for attorneys "appearing and practicing before" the SEC in the representation of issuers.[7] These complex and controversial rules require any such attorney who becomes aware of "evidence of a material violation"of federal or state law (or of a material breach of fiduciary duty) that has occurred, is occurring or is about to occur to report such evidence to the issuer's chief legal officer (or to its CLO and chief executive officer) "forthwith." If the reporting attorney does not receive an "appropriate response" within a reasonable time (or if the reporting attorney reasonably believes that reporting such evidence to the CLO and CEO would be futile), the reporting attorney must report the evidence to the audit committee, another committee of non-employee directors, or the full board.[8] The rules further provide that, in certain circumstances, the attorney may reveal confidential information to the SEC, without the issuer's consent, to prevent or rectify the consequences of such a material violation.[9]

The SEC rules only apply to attorneys appearing and practicing before the SEC in the representation of an issuer of publicly registered securities, and will therefore have no direct impact on private or nonprofit healthcare organizations. However, the concepts underlying them will likely influence perceptions as to how lawyers faced with potential corporate wrongdoing should behave, and even organizations not covered by the SEC rules may prudently consider adopting some type of formalized "reporting up" policy for counsel as a strategy to enhance corporate governance and compliance.

C. Rights and Responsibilities in the Court of Public Opinion

Of course, the Model Rules are only applicable if and when they are adopted by particular states, and the SEC rules do not apply to most healthcare organizations. However, when a corporate crisis emerges, the organization's lawyers are increasingly going to be judged based on evolving standards arising in light of the recent scandals. It is an imprudent in-house lawyer who assumes that he or she does not risk, at a minimum, a career-limiting decision by not being cognizant of the changing environment evidenced by the Model Rules amendments and the new and proposed SEC rules, even where they are not directly applicable. At the same time, in-house counsel must know and comply with the actual ethical and legal rules that apply to them in their particular practice setting and jurisdiction, notwithstanding prevailing policy considerations.

II. Key Considerations Before the Crisis Develops

Obviously, the best way to mitigate the effects of a crisis is to take steps well in advance to minimize the risk that a crisis will develop and to attempt to ensure that, if a crisis nonetheless emerges, the organization will be in the best position to discover the relevant facts quickly and respond to them at an early stage. This process should include establishing systems and lines of communication designed to reduce the risk that the organization's lawyers are put in a position that will require them to make an under-the-gun decision as to whether their professional responsibilities require such drastic steps as withdrawal, resignation or external disclosure. As part of this process, organizations should ensure regular communications between the general counsel and the board on matters of legal concern. In addition, organizations should focus on relationships within the legal department, between the legal department and the business people, and between inside and outside counsel.

A. Internal Relationships

1. Within the Legal Department

In a multi-lawyer legal department, the new environment makes it absolutely critical that the general counsel establish and maintain a policy whereby other lawyers in the department are encouraged and expected to bring material issues of concern to the general counsel. Whether the process is formal or informal, the general counsel must ensure that everyone in the reporting chain knows that they are expected to raise any issues that suggest potential violations by the organization or its agents and that such issues will be reviewed, investigated and addressed as necessary. Whatever the organizational structure, the key is to spread the message that up-the-ladder airing of issues within the department is not only welcome, but part of the job.

2. Within the Rest of the Organization

Just as important, in-house lawyers must maintain open communications with their business clients and make a genuine effort to stay informed of the business issues that they face and the goals they seek to achieve. The perpetual curse of the in-house lawyer is to be viewed as a "deal-killer," and the perpetual reaction of a business client faced with a deal-killer is to deprive the deal-killer of necessary information.

This attitude is extraordinarily dangerous in a healthcare organization, where many of the most economically compelling business strategies may run afoul of a wide variety of laws. In order to combat this attitude, and to obtain the information necessary to provide management personnel with appropriate guidance to prevent them from inadvertently stepping over the line, in-house counsel must build a relationship of trust and confidence with their business clients. Therefore, in-house lawyers should make it a priority to seek out time with their key internal clients in order

to be fully informed about their needs and concerns, and to try to provide the advice necessary to help them structure their arrangements in compliance with applicable laws. Developing these relationships will reduce the likelihood that the lawyer will have to confront any reporting up or reporting out decisions in a crisis, because the issues at the heart of the crisis will already have begun to be addressed.

B. Relationships between Inside and Outside Counsel

The organization's general counsel should review all counsel relationships and ensure that all outside counsel, whether reporting directly to the legal department or elsewhere in the organization, are made aware that the general counsel or other designated senior internal lawyers want and expect outside counsel to raise with them any concerns they may have about potential violations of the law or other compliance issues. The nature of these communications will depend on the specifics of the organization and the work assigned to outside counsel. However, all outside counsel serving the organization must understand that they have the opportunity and the responsibility to communicate material legal concerns to senior internal lawyers so that they can be addressed within the organization at an early stage.

III. When the Crisis Happens Anyway

Despite all enlightened precautionary steps, in-house counsel may still find themselves in the midst of a crisis. When that happens, internal counsel's ethical and professional responsibilities will be heightened, because the opportunity to rectify mistakes will be significantly lessened. Furthermore, if the crisis involves an alleged violation of laws by the organization or its agents, prior acts and advice of internal counsel may come under scrutiny, and such counsel will want to ensure that they avoid any activities that may be perceived as hindering or obstructing any investigations.

A. Engaging Appropriate Outside Help

While internal counsel will have a major role in the response to most legal-related crises, it is unlikely that internal counsel will, or should, want to go it alone. Time and resource limitations will make it difficult for internal counsel to fulfill their regular duties and respond to the demands of the crisis. Further, where the crisis involves governmental and law enforcement agencies, it is highly advisable to bring in outside counsel who have appropriate relationships with the relevant entities and are experienced in dealing with them in crisis mode. In a corporate crisis, there is limited opportunity to recover from strategic missteps and inadvertent errors (for example, in responding to the extensive document requests that invariably accompany an investigation). Counsel experienced in such situations are invaluable team members.

Of course, senior internal lawyers should play a key role in coordinating the effort, ensuring that the efforts of outside lawyers are appropriately directed and facilitated and maintaining the flow of communication with management and the board. However, as a matter of both effective crisis response and professional responsibility obligations to the organization, internal counsel will normally want to ensure that appropriate outside professionals are associated early.

B. The Challenge of Multiplicity

In addition to counsel for the organization itself, some types of corporate crises will involve a variety of other outside lawyers. In a major crisis potentially implicating senior management, the board of directors, the outside directors, the audit committee, etc., may feel the need to bring in their own independent counsel. The general counsel should be prepared to advise directors on such action and to work cooperatively with any separate independent counsel that are retained.

Where individual corporate employees are potentially involved (and especially where they have been identified as targets of the investigation), it may be necessary for them to engage separate counsel. In such a case, it will be necessary to review applicable law, the organization's governing documents, applicable employment and indemnification agreements, and any other established corporate policies to determine whether the organization may, or is required to, cover the costs of such counsel. Because the affected employees are likely to be persons with whom internal counsel has a working and/or reporting relationship, it is highly advisable for internal counsel to seek outside counsel's assistance in evaluating these issues and making recommendations to the board. Similarly, outside counsel can play a key role when the organization is pressured to disregard potential indemnification and advancement obligations for fear of antagonizing prosecutors or incurring negative public perceptions of "supporting the bad guys." Such involvement of outside counsel will help internal counsel avoid any perception of undue self-interest in these decisions.

C. The "Unfortunate Discovery"

At the beginning of an investigation, counsel may reasonably believe that the investigators have the facts wrong and/or that there are colorable defenses to the claims. At some point, however, there may be the unpleasant discovery of really bad facts – the smoking gun e-mail, the memo from senior management apparently sanctioning a violation of the law, the lower-level employee who claims to have been directed to commit a fraud. What then becomes the professional responsibility of the internal lawyer, and what role should outside counsel play?

Internal counsel faced with such disturbing information should first investigate and evaluate it in a reasonable and appropriate manner, taking into account all available relevant information and its impact on the organization's legal position. If the matter is serious, internal counsel will likely find it prudent to involve outside counsel, both for the benefit of additional analysis and to avoid any perceived conflicts of interest.

If the results of such evaluation indicate that agents of the organization have engaged in illegal behavior, internal counsel (with or without the assistance of outside counsel) will normally want to address the matters with the individual agents involved and encourage them to take appropriate remedial steps, including bringing the matter to the attention of their own superiors.

Where that approach has been ineffective, or where the lawyer reasonably believes it would be futile or inappropriate, the lawyer should proceed up the ladder to bring the matter to the attention of appropriate levels of senior management, and, if necessary, the board of directors. This does not mean that the lawyer should always assume the role of final arbiter of what the organization's appropriate response should be. The questions of whether an organization's agents have violated the law and of what the organization's response should be are frequently not black-and-white, especially in the world of healthcare law. The lawyer's duty is to advise management and the board of the legal issues involved so that they can make an informed decision on how to respond to them. Absent unusual circumstances, the lawyer's duties do not extend to "overruling" valid, informed decisions made by the organization's management and board. The involvement of outside counsel can help ensure that those in the up-the-ladder chain are fully informed of the issues and have an appropriate basis for their decisions.

Finally, what if the organization persists in a course of action that internal counsel believes constitutes (or continues, or covers up) a violation of the law even after up-the-ladder reporting? At the moment, neither the Model Rules nor the SEC rules require disclosure outside the organization, nor do most currently existing state ethics rules. However, the lawyer cannot knowingly aid or abet violations of the law by the organization, and a lawyer who knows of such violations must carefully consider his or her rights or obligations under specifically applicable laws and ethical rules and take such steps as he or she reasonably believes are in the best interests of the organization. While the lawyer's rights and obligations in such a situation are highly fact-dependent, any lawyer facing such a situation must be prepared to make, and justify, difficult decisions or face substantial potential personal exposure. Indeed, inside counsel may well benefit from consulting with his or her own "lawyer's lawyer" to help ensure compliance with such counsel's duties.

IV. Conclusion: "Let's Be Careful Out There"[10]

In the past, many lawyers may have assumed that if they were reasonable and cautious in the advice they rendered and the services they provided, they were relatively insulated from scrutiny and potential liability even if their clients committed wrongdoing. With today's heightened focus on corporate responsibility, that notion, if it was ever valid, can now only be regarded as providing a sense of false security. Lawyers simply cannot afford to ignore the concerns underlying the new focus on lawyers as "gatekeepers" for their clients, even where those concerns are not entirely consistent with applicable professional responsibility rules.

This is particularly true for in-house counsel. There is a growing sense in many quarters that in-house counsel have some generalized oversight responsibility in their organizations that causes them to be, at some level, responsible for any failure to detect and remedy wrongdoing within those organizations, however it may arise. Thus, it is critical for in-house lawyers to stay abreast of the current general developments in professional responsibility and to stay informed of the particular legal requirements and ethical rules applicable to their particular practice setting and jurisdiction.

As discussed above, outside counsel can provide useful assistance in this endeavor in several ways. Thus, as with so much of the in-house practice, professional responsibility is an area where informed teamwork between inside and outside counsel can avoid or mitigate much trouble.

William W. Horton practices corporate, securities and healthcare law with Haskell Slaughter Young & Rediker, LLC, with offices in Birmingham and Montgomery, Alabama and New York City. He previously served as general counsel of HEALTHSOUTH Corporation and holds leadership roles with the American Health Lawyers Association and the American Bar Association's Health Law Section. Mr. Horton may be reached at wwh@hsy.com.

1 See MODEL RULES OF PROF'L CONDUCT R. . 1.6(b)(3)–(4) (2004).
2 MODEL RULES OF PROF'L CONDUCT R. 1.13(b) (2004).
3 See MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(3)–(4) (2004).
4 MODEL RULES OF PROF'L CONDUCT R. 1.13(b) (2004).
5 MODEL RULES OF PROF'L CONDUCT R. 1.13(c) (2004).
6 15 U.S.C.A. § 7245 (2003).
7 17 C.F.R. pts. 205.1 – 205.7 (2004). See U.S. Sec. & Exch. Comm'n, Final Rule: Implementation of Standards of Professional Conduct for Attorneys (Jan. 29, 2003), *available at* www.sec.gov/rules/final/33-8185.htm.
8 See 17 C.F.R. § 205.3(b).
9 *Id.* § 205.3(d)(2).
10 Sgt. Phil Esterhaus, *Hill Street Blues* (NBC-TV).

Rapid response. Gordon Apple, of the Law Offices of Gordon J. Apple PC, Saint Paul, Minn., noted that complaints must be filed within 180 days of when the complainant knew or should have known the act or omission occurred. The good news, he said, is the entity can find out about the problem and "fix things right away." Yet with the HIPAA process moving so quickly, he said, "There is a potential you'll have to deal with a record." Almost all investigations will start from a compliant, he said, with the remainder resulting from compliance reviews.

HIPAA (cont.)

Covered entities should make sure they are in contact with their affiliated covered entities if they want to stay up to date, said Apple. Each covered entity that is a member of an ACE would be jointly and severally liable for a CMP for a violation by the ACE, he noted. With respect to affiliated covered entities, Apple advised: "Make sure there is effective oversight of all these different groups." He noted that this step will help covered entities respond quickly once a compliant comes in. "You really cannot afford to have any weak links with respect to your ACE organizations so that you know when a complaint has been made."

Finally, Apple advised covered entities to resolve complaints and investigations fast. "You want to be in a position of settling these things as soon as possible," he said. He recommended covered entities investigate complaints and violations promptly. "You need to know as quickly as possible what happened," he said. ■

Trends

Ways and Means Committee looks at exempt orgs

by CCH Editorial Staff

At a standing-room-only hearing in Washington, D.C., House Ways and Means Committee Chairman William M. Thomas, R-Calif., said that there has been no comprehensive oversight of the tax-exempt sector by Congress in nearly 20 years. The hearing looked at a broad overview of the laws governing the tax-exempt sector, with an eye toward how organizations operate, how laws are administered and what impact they have on the lives of American taxpayers.

Thomas noted that many goods and services provided by tax-exempt organizations are similar – if not identical – to goods and services provided by taxpaying entities. "This raises the fairly fundamental question of what makes these organizations unique and, hence, deserving of a tax-exempt status, he said."

Congressional Budget Office Director Douglas Holtz-Eakin testified that nonprofit institutions, such as hospitals, credit unions, and universities, may control untaxed business entities that compete with for-profit companies. He said that the main difference is that these entities do not have shareholders who profit from the success of these untaxed businesses. As a result, managers have incentives to lower prices, increase costs or bolster retained earnings.

"Accordingly, taxation of these entities might not generate as much revenue as initially anticipated," Holtz-Eakin said. "Taxation would bolster managers' incentives to reduce or eliminate entities' tax liabilities by using more of any surplus to cut prices, boost costs or both." If taxed, these entities would retain fewer funds for expansion, he said.

Continued oversight of the tax-exempt sector is critical to ensuring that entities operate with integrity in meeting their mission, according to General Accounting Office Comptroller General David M. Walker. The IRS has begun to increase staff, obtain better data and better analysis of that data, Walker said in his testimony.

Walker called for a comprehensive reexamination of the nonprofit sector to determine whether tax-exempt entities are providing services commensurate with their favored tax status and whether the current number and nature of exemptions continue to make sense. ■

CCH Washington Bureau, May 16, 2005

Nonprofit medical center entitled to exemption

by CCH Editorial Staff

A nonprofit medical center that owned an office building in which it leased office space to private physicians was entitled to a Louisiana local property tax exemption (*Willis-Knighton Medical Center v. Edminston*, Louisiana Appellate Court, Second Circuit, April 6, 2005).

The assessor contended that the leasing of the office space was not related to the taxpayer's exempt purpose because the physician tenants only referred a fraction of their patients to the taxpayer and 60 percent of the building was leased to or owned by for-profit entities. However, the evidence demonstrated that the physicians who leased office space were members of the taxpayer's medical staff and used the office space for the examination and treatment of patients. Accordingly, the leasing of the office space was a commercial purpose reasonably related to the taxpayer's exempt purpose of delivering medical care to individuals. ■

CCH Chicago Bureau, May 16, 2005