CCH Health Care Compliance LETTER

Volume 8, Issue 4 health.cch.com February 21, 2005

OIG addresses hospital-surgery group cost savings arrangement

by Anuradha Gupta, JD, Contributing Editor

The Office of Inspector General (OIG) determined that a proposed cost savings arrangement between an acute care hospital and a professional cardiac surgery group could potentially result in improper payment implicating the civil money penalty (CMP) and the anti-kickback statute under the Social Security Act (the Act).

Under the arrangement, the hospital would pay the surgeon group 50 percent of the first-year cost savings directly attributable to specific changes in the surgeon group's operating room practices. The measurement of cost savings would be based on the surgeons' use of specific supplies during designated cardiac surgery procedures. According to the program administrator, twenty-four specific cost savings opportunities were identified that should not adversely impact the quality of patient care. These opportunities were roughly grouped into the following four categories:

1. opening packaged items only as needed during a procedure;
2. performing blood cross-matching only as needed;
3. substituting, in whole or part, less costly items for the items currently being used by the surgeons; and
4. product standardization of certain cardiac devices where medically appropriate.

The OIG review concluded that nearly all of these cost savings opportunities implicate the CMP section of the Act by constituting an inducement to reduce or limit the current medical practice at the hospital. Because the proposed agreement provides sufficient safeguards, however, the OIG would not seek sanctions under the Act. In addition, these safeguards reduce the likelihood that the arrangement will be used to attract referring physicians or to increase referrals from existing physicans. Accordingly, the OIG concluded that (1) sanctions would not be imposed on the requesters in connection with the proposed arrangement even though it would constitue an improper payment to induce reduction or limitation of services; and (2) the proposed arrangement would potentially generate prohibited remuneration under the anti-kickback statute, if the requisite intent to induce or reward referrals of federal health care program business were present, but sanctions would not be imposed in the particular cirumstances presented in this case. ■

OIG Advisory Opinion No. 05-01, ¶500,123

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.

Supplemental guidance for hospitals provides blueprint for compliance success

by Gené Stephens, JD, Contributing Editor

The Office of Inspector General (OIG) recently issued its Supplemental Compliance Program Guidance for Hospitals (CPG). Realizing the diversity of the hospital industry, the OIG's CPG does not provide a "one-size-fits-all" guidance, but rather encourages hospitals to identify and focus their compliance plans and efforts on areas of potential concern and risk that are the most relevant to their individual organizations and to the delivery of health care in general. The OIG explained that hospitals may gain important information by voluntarily implementing a compliance program that includes: (1) a demonstration of the hospital's commitment to honest and responsible corporate conduct; (2) a plan of increasing the likelihood of preventing, identifying and correcting unlawful and unethical behavior at an early stage; (3) a method of encouraging employees to report potential problems to allow for appropriate internal inquiry and corrective action; and (4) a plan that, through early detection and reporting, minimizes any financial loss to government and taxpayers, as well as any corresponding financial loss to the hospital.

The OIG emphasized several problematic areas that hospitals have identified in managing health care service delivery systems. The CPG places particular emphasis on the areas of: (1) fraud and abuse; (2) hospital compliance program effectiveness; (3) hospital adherence to anti-kickback safe harbor protections; (4) use of information technology in the hospital setting; and (5) voluntary, self-reporting of compliance risk areas.

Common business arrangements. The CPG provides hospitals with a two-part inquiry test when analyzing business arrangements or practices under the anti-kickback statute. Specifically, the OIG recommends that hospitals ask:

- Does the hospital have any remunerative relationship between itself (or its affiliates or representatives) and persons or entities in a position to generate federal health care program business for the hospital (or its affiliates) directly or indirectly? This includes persons or entities in a position to generate federal health care program business for a hospital, including, for example, physicians and other health care professionals, ambulance companies, clinics, hospices, home health agencies, nursing facilities, and other hospitals.

"The OIG emphasized several problematic areas that hospitals have identified in managing health care service delivery systems."

- With respect to any remunerative relationship identified, could one purpose of the remuneration be to induce or reward the referral or recommendation of a business payable in whole or in part by a federal health care program?

The CPG suggests that hospitals take a number of steps to reduce or eliminate the risk of an anti-kickback violation and provides a list of the most relevant safe harbors. The OIG recommends that hospitals structure business arrangements to fit within applicable safe harbors and to evaluate arrangements that do not fit into a safe harbor on a case-by-case basis.

Joint ventures. The language of the CPG reiterates the OIG's long-standing concern about joint venture arrangements between persons and entities in a position to refer or generate federal health care program referral business and those providing items or services reimbursable by federal health care programs. The CPG provides hospitals with several factors to consider when scrutinizing joint ventures under the anti-kickback statute, including: (1) the manner in which the joint venture participants are selected and retained; (2) the manner in which the joint venture is structured; and (3) the manner in which investments are financed and profits are distributed.

Compensation arrangements with physicians. The OIG provides a few general "rules of thumb" for hospitals when entering into compensation arrangements with physicians who provide items or services to, or on behalf of, the hospital. The CPG explains that any remuneration flowing between hospitals and physicians should be at the fair mar-

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
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 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.

Fraud & Abuse (cont.)

ket value for any actual and necessary items furnished or services rendered based upon an arm's-length transaction. The arrangement should also take into account the value or volume of any past or future referrals or other business generated between the parties.

Information technology. As part of its emphasis on accurate billing and coding, the OIG reminds hospital administrators of the industry's increasing reliance on information technology as it moves forward. Particular attention is given to the HIPAA Privacy and Security rules regarding electronic claims submissions, electronic prescribing, networked information sharing among providers, and system tracking and reduction of medical errors. The OIG suggests that prudent hospitals take steps to ensure that they thoroughly assess all new computer systems and software that might impact coding, billing or the transmission and generation of health care information.

Stark provisions. Equally as important and emphasized by the OIG is the due diligence that hospitals must provide when reviewing all financial relationships with referring physicians for compliance with the recent changes to the Stark law. The OIG provides hospitals with a three-question inquiry for analyzing financial relationships under Stark that it believes will be helpful for hospital compliance professionals. Specifically, the OIG recommends that hospitals ask: (1) if there is a referral from a physician for a designated health service; (2) whether the physician (or an immediate family member) has a financial relationship with the entity furnishing the designated health service; and (3) whether the financial relationship fits within one of the Stark exceptions.

Finally, the OIG provides some guidance on the treatment of providers and suppliers who provide discounts to uninsured or under-insured patients exclusion and provides additional assurances to the industry that, historically, providers have not been excluded for providing discounts to uninsured individuals. Hospitals would be wise to incorporate the CPG's guidance policies into their existing corporate governance and compliance programs. ■

OIG Supplemental Compliance Program Guidance for Hospitals, January 2005, ¶510,017

Safety

OSHA offers Best Practices for hospitals receiving victims of mass casualties

by CCH Editorial Staff

The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) has released information to help hospitals safeguard their own employees as they care for patients injured in incidents involving chemical, biological or radiological materials.

Entitled "OSHA Best Practices for Hospital-Based First Receivers of Victims from Mass Casualty Incidents Involving the Release of Hazardous Substances," the document is available on OSHA's Web site and offers useful information to help hospitals create emergency plans based on worst-case scenarios. It focuses on suggestions for appropriate training and suitable personal protective equipment for healthcare employees who may be exposed to hazardous substances when they treat victims of mass casualties. The document includes appendices with practical examples of decontamination procedures and medical monitoring for first receivers who respond to a mass casualty incident.

To develop the guidance, OSHA drew upon the best practices of hospitals of varying sizes and with differing risk levels and conducted an extensive literature search. The agency also placed a draft on its Web site during August 2004 and solicited additional stakeholder input.

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) requires hospitals to develop plans to respond to both natural and manmade emergencies. Depending on their roles, some hospital employees also may be covered by OSHA's hazardous waste operations and emergency response standard. Following the guidance in the document will enable hospitals to fulfill these responsibilities.

OSHA's best practices document for first receivers is available at http://www.osha.gov/index.html on the Emergency Preparedness and Response Web page. ■

CCH Chicago Bureau, February 11, 2005

On The Front Lines

HIPAA issues in health care transactions

by W. Andrew H. Gantt, III, and Anthony B. Casarona

The HIPAA Privacy Rule has had a notable impact on the manner in which health care transactions that involve the "covered entities" regulated by HIPAA are conducted. The Privacy Rule's restrictions on the flow of protected health information (PHI) create a host of unique considerations and concerns for parties to any sale, merger, acquisition or other corporate transaction involving one or more covered entities.

Use and Disclosure of PHI in Health Care Transactions

Preserving the Ability to Transfer PHI

As a threshold matter, a covered entity should ensure that it preserves the right to sell PHI, if it ever intends to do so, whether in the context of a sale of all or part of its business. For many covered entities, PHI contained in such varied forms as patient lists, databases of clinical trial information and accounts receivable information, may constitute the covered entity's most valuable assets. However, covered entities do not always take steps necessary to preserve the right to transfer such PHI, and may even take deliberate steps that can jeopardize this right.

The Privacy Rule requires a covered entity to have a "notice of privacy practices." Such notice includes a description of the types of uses and disclosures of PHI the covered entity may make (consistent with the Privacy Rule's requirements) and establishes the standard by which the covered entity's activities will be measured. This description in the covered entity's notice of privacy practices should include a statement that PHI may be used or disclosed in connection with the sale of all or part of its business. Moreover, the covered entity should ensure that any other privacy policy the covered entity may establish, such as on such entity's website, similarly preserves this right. So as to mitigate the public's concerns regarding the use of PHI in marketing activities, many companies have made the mistake of asserting that they will never sell a patient's information without that patient's prior authorization, unwittingly preventing those companies from transferring such information upon the sale of all or part of their business in a manner that might otherwise be permitted under the Privacy Rule.

Restrictions on Transfer of PHI

As a general matter, unless one of the specific exceptions set forth in the Privacy Rule is satisfied, prior patient authorization is required to use and disclose PHI. The administrative burden of acquiring individual authorizations from each individual whose medical records are maintained by a covered entity and segregating the records of those individuals who refused to provide an authorization would, in most cases, be impractical. Accordingly, the covered entity's ability to meet an exception to the general rule is critical to the exchange of PHI in the context of a health care transaction.

Under one exception to the Privacy Rule, a covered entity may use and disclose PHI without patient authorization for purposes of treatment, payment, or health care operations.[1] The health care operations exception is critical to a covered entity's ability to disclose PHI in health care transactions. A covered entity's health care operations include, among other things:

- the sale, transfer, merger or consolidation of all or part of the covered entity to or with another covered entity, or an entity that following such activity will become a covered entity; and
- due diligence related to such activity.[2]

When discussing the scope of permissible health care operations, the Department of Health and Human Services (HHS) has explained that this definition includes both the use and disclosure of PHI to conduct due diligence and the actual physical transfer of patient records upon the consummation of the transaction.[3] The following example provided by HHS provides further clarity to the intent of the agency in adopting this provision of the Privacy Rule:

> if a pharmacy which is a covered entity buys another pharmacy which is also a covered entity, [PHI] can be exchanged between the two entities for purposes of conducting due diligence, and the selling entity may transfer any records containing [PHI] to the new owner upon completion of the transaction. The new owner may then immediately use and disclose those records to provide health care services to the individuals, as well as for payment and health care operations purposes. Since the information would

continue to be subject to the Privacy Rule, any other use or disclosure of the information would require an authorization unless otherwise permitted without authorization by the Rule, and the new owner would be obligated to observe the individual's rights of access, amendment, and accounting.[4]

Thus, the agency's position attempts to strike a necessary balance between the realities of corporate transactions and maintaining the privacy of patients' medical records.

However, many health care transactions are not as simple as the HHS example and not easily addressed given the dearth of guidance regarding the application of this exception to various health care transactions. In particular, disclosures of PHI to individuals or entities that are not and would not, as a result of the transaction, become covered entities are not included in the definition of health care operations. For example, it is not clear that this exception would apply where a covered entity would seek to disclose PHI to multiple bidders who are not covered entities (e.g., private equity or venture capital firms) in the context of a competitive bid to acquire the covered entity, where only one of the bidders will consummate a transaction and become a covered entity. Moreover, it is not clear that this exception would allow PHI to be shared with affiliates of the acquiring party or with entities serving the acquiring party (e.g., law firms, accountants advisors, and sources of financing) in the transaction before the acquiring party becomes a covered entity.

Disclosures of PHI by the covered entity to its advisors in the context of a deal are permitted, provided the covered entity enters a business associate agreement meeting the Privacy Rule's requirements with each advisor. Such agreement requires these entities that are not otherwise subject to the Privacy Rule to contractually agree to comply with many of its provisions.

In addition, even where disclosure of PHI is permitted by the Privacy Rule, there are other constraints that complicate health care transactions. Notably, like most other uses and disclosures of PHI, uses and disclosures for health care operations are subject to the so-called "minimum necessary" rule. This rule requires a covered entity to reasonably limit the PHI that it uses and discloses and that it requests from another covered entity to the minimum amount of information necessary to accomplish the intended purpose of the use, disclosure or request.[5] Accordingly, even where disclosure is permitted, such as in the due diligence process, the covered entity disclosing PHI must assess what constitutes the minimum amount of PHI necessary to permit the recipient to conduct due diligence.

Other Restrictions

Notwithstanding the latitude afforded to covered entities under the Privacy Rule for health care operations, uses and disclosures under this provision are not without risk. For example, HHS has emphasized that even if a covered entity complies with the health care operations rule, it must still be mindful of other "legal or ethical obligations" that may arise out of the nature of its business or relationship with customers or patients.[6] This is significant because the Privacy Rule merely establishes a uniform federal floor for protecting the privacy of PHI, but does not preempt state laws that are more protective of the privacy of individuals' medical records. As a result, before engaging in uses or disclosures of PHI otherwise permitted under the Privacy Rule as health care operations, covered entities must identify state laws which limit the manner in which such uses and disclosures may be made. Examples of such state laws include those requiring notice of an impending transfer of PHI to affected individuals and an opportunity to object, or which prohibit transfers altogether in the absence of a signed authorization or other mandatory form of consent.

In addition, the Privacy Rule permits an individual to request that a covered entity restrict routine uses or disclosures that the covered entity may make about the individual, including those made under the guise of health care operations.[7] Although the rule does not require a covered entity to agree to these requests, if the entity does, it could be exposed to liability for violation of the agreed-upon restrictions.

Conducting Privacy Rule Due Diligence

In addition to imposing restrictions on the disclosure of PHI in health care transactions, the Privacy Rule creates a need for due diligence of the target covered entity's compliance with the Privacy Rule's various organizational and administrative requirements. Each covered entity and each transaction will present unique issues that must be addressed in due diligence. However, at a minimum, the due diligence review should verify that the covered entity has taken the following measures:

- preserved the ability to transfer PHI in connection with the proposed transaction;
- designated a privacy officer who is responsible for developing and implementing its privacy policies and procedures, overseeing workforce training, and addressing complaints involving the covered entity's use and disclosure of PHI;
- developed and implemented written privacy policies and procedures consistent with the Privacy Rule which demonstrate that the covered entity has in place appropriate administrative, technical and physical safeguards to prevent the use or disclosure of PHI in violation of the Privacy Rule;
- trained and periodically retrained members of its workforce

on its privacy policies and procedures as necessary for them to perform their employment functions;
- implemented procedures addressing the provision of access, amendments to, or an accounting of disclosures of PHI that it maintains;
- entered into business associate agreements, as necessary, with third parties performing services on its behalf;
- prepared and disseminated a HIPAA-compliant notice of privacy practices;
- has and uses when required, a HIPAA-compliant form of authorization;
- implemented a system to document uses and disclosures of PHI, the disposition of complaints involving the use or disclosure of PHI, and to maintain its privacy policies and procedures, notice of privacy practices and other related items as required by the Privacy Rule;
- if the covered entity maintains PHI in electronic format, established (or will have in place no later than April 21, 2005) safeguards, as required by the HIPAA Security Rule,[8] to protect against reasonably anticipated threats or hazards to the security and integrity of electronic PHI, including having in place an information systems infrastructure capable of ensuring that these safeguard are consistently employed; and
- if the covered entity engages in standard transactions addressed in the HIPAA Transactions Rule,[9] implemented appropriate policies for the proper processing of these transactions, including ensuring compliance by third parties engaged to process these transactions on the covered entity's behalf.

In any transaction, if the target covered entity has not undertaken these basic obligations, it will become necessary to include the cost of post-closing compliance efforts in assessing the economic benefits of the transaction. Beyond diligence of the covered entity's basic compliance efforts, the due diligence effort should include a review of the covered entity's complaint history and any litigation relating to privacy issues, as well as any contractual arrangement under which the covered entity has agreed to indemnify third parties for its failure to comply with HIPAA. An acquirer must carefully assess the potential liability that it will incur as a result of the covered entity's compliance deficiencies and the costs likely to be incurred to ensure compliance after the transaction is consummated, and determine how such liability should be reflected in the terms of the deal documents.

The Ongoing Impact of the Privacy Rule

The Privacy Rule's impact on transactions involving covered entities does not end with a signature on the dotted line. These transactions will frequently be subject to post-closing indemnification and other related obligations that may require the use or disclosure of PHI between an individual or entity and its successor in interest. In many cases, a business associate agreement will be necessary in order to ensure that these obligations do not run afoul of the requirements of the Privacy Rule. In addition, the Privacy Rule may require business associate agreements with lenders who hold a security interest in accounts receivable or who maintain rights of audit and inspection under credit and related agreements if these rights will expose the lenders to PHI. The obligations of being a business associate could present risk management, operational and financial concerns for a lender who is not familiar with the Privacy Rule or accustomed to the requirements imposed upon business associates.

Conclusion

The inception of the Privacy Rule resulted in a fundamental shift in the way that covered entities use and disclose PHI. As a result, covered entities now must expend considerable time and resources to ensure that their activities do not expose them to potential civil and criminal liability. These concerns are not without significance for individuals and entities involved in corporate transactions involving covered entities. Under the paradigm created by the Privacy Rule, parties to a transaction must be mindful of the rule's provisions and also of the consequences, economic and otherwise, of both compliance and non-compliance. From understanding the conditions under which PHI may be transferred and used for due diligence purposes, to the evaluation of an entity's compliance activities and potential liability exposure, to post-closing operational issues, the Privacy Rule has injected an entirely new set of issues that must be addressed by all parties, whether or not they are covered entities, in connection with transactions involving entities in the health care industry.

Andrew Gantt is a partner in Latham & Watkins' Washington, DC, office, where he is a member of the firm's Health Care Practice Group. Mr. Gantt represents a wide variety of health care providers, manufacturers, suppliers and health care e-commerce companies in corporate and regulatory matters, including compliance with the Health Insurance Portability and Accountability Act of 1996. In addition, Mr. Gantt advises venture capital groups, private equity funds and underwriters on a variety of health care regulatory issues in connection with health care transactions.

Anthony Casarona is an associate in Latham & Watkins' Washington, DC, office, where he is a member of the firm's Health Care Practice Group. Mr. Casarona provides corporate, transactional, and regulatory advice to a wide range of individuals and entities involved in the health care industry. In addition, Mr. Casarona represents health care service providers in matters related to their compliance with the Health Insurance Portability and Accountability Act of 1996.

1 45 C.F.R. § 164.502(a).

2 *Id.* at § 164.501.

3 Standards for Privacy of Individually Identifiable Health Information; Final Rule, 67 Fed. Reg. 53182, 53190 (Aug. 14, 2002).

4 *Id.* at 53190-91.

5 45 C.F.R. § 164.502(b).

6 67 Fed. Reg. at 53191.

7 45 C.F.R. § 164.522(a).

8 45 C.F.R. Part 160 and Part 164, Subpart C.

9 45 C.F.R. Part 162.

Preparing for disasters: How to develop a HIPAA contingency plan

by Catherine Hubbard, MA, Contributing Editor`

Computer systems are never a hundred percent reliable. They can crash, making data difficult, if not impossible, to recover. Under the HIPAA Security Rule, which covered entities must start complying with in April, health care companies must develop a data backup plan. "It is important to backup electronic data," said Walt Culbertson, CEO and President, HealthTransactions, Inc., Jacksonville, Florida, during a February 9 audio conference sponsored by the Centers for Medicare & Medicaid Services and the SharpWorkGroup.

Health care organizations must establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information and backup data on a regular basis, said Culbertson. He noted that while it's relatively easy to reinstall computer programs, it can be virtually impossible to recreate the covered entity's data.

One occasion when it's particularly important to create a backup is before moving equipment, Culbertson noted. "It is especially important to ensure information is backed up prior to moving any equipment, as information may be lost or equipment impaired during movement," he said, suggesting companies keep an extra copy of backed-up data in a secure manner and at a different geographic location in case there is a disaster at the main location.

Organizations must also establish, and implement as needed, procedures to restore any lost data, Culbertson said in prepared materials. "A covered entity must have plans to recover and restore data in the case of any disaster," he emphasized.

However, it may not be critical to restore all the covered entity's information immediately, said Culbertson, noting that the only time information must be available continuously is when the temporary loss of such information could threaten a patient's health. "In most instances this is not the case and a covered entity can wait a day or a few days before it absolutely has to have its systems back up and running," he said. By then the disaster, such as a power outage, may have passed, he added.

Emergency planning. HIPAA also requires covered entities to implement an emergency mode operation plan containing procedures that enable them to continue critical business processes that protect the security of electronic protected health information, Culbertson said.

"Health care organizations must establish and implement procedures to create and maintain exact retrievable copies of electronic protected health information and backup data on a regular basis."

"This may be as simple and maintaining paper records until the emergency situation is over," he said.

Contingency plans need to be tested and revised regularly, said Culbertson. "You should review your contingency plans on an established periodic basis, or when the structure (physical or operation) of your organization changes," he said. Initially, testing should be done in sections or functional areas or departments and during non-operations hours, he added.

Covered entities also need to review and document the relative importance of all software, hardware and applications, Culbertson said. For example, he said, if a covered entity uses two applications, one for scheduling and one for accessing certain electronic PHI, it should consider which one is more critical or important to restore first in the event of an emergency. "The order of priority will be very important in creating the detailed backup, disaster recovery and emergency mode operations," he said.

Also crucial, is establishing procedures that allow support personnel to get into the facility and restore lost data in the event of an emergency. This will help ensure those needing access in an emergency have access, including any individuals who normally do not have access to the covered entity's electronic information, Culbertson said.

The primary objectives of a disaster recovery plan are to protect the organization in the event that all or part of its operations and/or computer services are rendered unusable, minimize disruption of operations and ensure some level of organizational stability and an orderly recovery after a disaster, Culbertson said. "Preparedness is the core element of the plan," he said. Culbertson noted that covered entities must identify potential threats to the organization and plan for continuing operations in an emergency.

Moreover, a disaster recovery plan provides a sense of security, minimizes the risk of delays, guarantees the reliability of standby and secondary systems and processes, establishes a standard plan for testing and minimizes decision making during a disaster, Culbertson said.

"Disaster recovery is not a new priority for the healthcare industry," said Culbertson. "Experienced managers have long known that not all disasters come in a form as dramatic as an earthquake or a hurricane," he said, noting that power outages and telecommunications breakdowns are common causes of disruptions.

The bottom line is be prepared. "Being prepared for both human, technology and natural disasters is of utmost importance in terms of both patient care and organizational survival," Culbertson said. ■

CCH Washington Bureau, February 15, 2005

Expert outlines steps for protecting EPHI

by Catherine Hubbard, MA, Contributing Editor

Health care organizations will need to conduct thorough risk assessments of their buildings, computer systems, and workstations to prevent security breaches and comply with the HIPAA Security Rule, according to Mary Rita Hyland, Assistant Vice President of the SSI Group, Inc., Mobile Alabama. "Know where your PHI resides," she said at a January 26 audio conference sponsored by the Centers for Medicare & Medicaid Services (CMS) and the SharpWorkGroup.

Covered entities will need an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (EPHI) held by the covered entity, said Hyland in prepared slides. She recommended that organizations conduct a thorough assessment of employees' workstations and of any portable devices, such as laptops, PDAs, USBs, cell phones or wireless networks.

Covered entities also should create an inventory of all their systems that maintain electronic protected health information. "Perform an evaluation of each system to determine HIPAA compliance," she suggested. Organizations should find out whether the systems have audit trails, timeout functions and whether they are managing who has access to the systems, she said.

The final HIPAA Security Rule, published on February 20, 2003, carries a compliance date of April 20 for all covered entities except small health plans, which have one more year to comply.

Physical safeguards. Organizations are required to protect their electronic information systems and EPHI from unauthorized physical access while permitting properly authorized access. Noting that physical safeguards is an addressable item, Hyland pointed out that organizations can decide whether to institute low or high control levels.

Under a low security system, for instance, all physical access points would be controlled through the use of locks during working hours and guarded or locked during non-work hours. Raising that up a notch, a moderate system would control all physical access points twenty-four hours per day, seven days per week through the use of entry devices such as key cards or biometrics, she said. In a high security system, all physical access points would be controlled 24/7 through the use of guards or monitored alarms.

Covered entities must implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision, said Hyland. She noted they can protect access to critical workstations and servers by utilizing an effective physical access control method. "This will protect critical systems and information from unauthorized users who are allowed access to physical devices," she said.

The organization needs to establish what tasks can be performed at each workstation, the manner in which tasks can be performed and the physical attributes of areas where workstations with access to EPHI are located, Hyland said. Covered entities should ask whether any servers, routers and telecommunications are located in non-locked publicly accessible or department-wide accessible locations; whether all distributions of badges and passkeys are recorded on a paper log or in a database; whether all public traffic in and out of the facility is controlled and monitored by a security guard, receptionist or video surveillance; and whether administrator passwords are commonly known in an office setting.

Hyland recommended that organizations segregate job duties so that people do not have access to a complete system, application or information set. She also suggested companies tie employees' duties to their access (role-based access), use two-factor authentication on remote access and to critical information (user ID, password and smart card or key) and limit access to Internet sites.

Device and media controls. In addition, Hyland said covered entities must develop and implement policies and procedures for the receipt and removal of hardware and electronic media that contain EPHI into and out of an organization and the movement of those items within and out of the covered entity. They also must implement policies and procedures designed to eliminate electronic PHI from all media before that media is made available for re-use. Moreover, they must maintain a record of the movements of hardware and electronic media and any person responsible for the move, and they must create a retrievable, exact copy of EPHI, when needed, before movement of equipment, she said.

Physical computer systems and related buildings and equipment also need to be protected from fire and other natural and environmental hazards, as well as from intrusion, Hyland outlined. These protections should include use of locks, keys and administrative measures to control access to computer systems and facilities, she said, recommending organizations assign security responsibility to a specific individual or organization.

Physical access controls must include procedures for verifying access authorizations before granting physical access, procedures to sign in visitors, testing and revision, secure workstation location, disaster recovery, emergency mode operation, equipment control, a facility security plan, maintenance records and need-to-know procedures for personnel access, Hyland said.

"Security is about people, not technology," said Hyland. "Security is everyone's job," she said, adding that understanding regulations pertaining to their job "is critical." ■

CCH Washington Bureau, February 14, 2005