CCH Health Care Compliance LETTER

Volume 11, Issue 17 health.cch.com August 19, 2008

CMS finalizes several changes in Stark regulations

CMS has finalized several Stark regulation revisions that have been proposed in different rules over the last year, as part of the fiscal year (FY) 2009 inpatient hospital prospective payment system (IPPS) update. The final rule is scheduled to publish in the Federal Register on August 19, 2008.

Physician-owned hospitals. CMS is expanding the definition of "physician-owned" hospital to include hospitals in which an immediate family member of a physician has an ownership or investment interest. Physician-owned hospitals that currently have no referring physicians on staff, however, will be exempt from the requirement to disclose to patients that it is physician-owned.

CMS also has clarified the regulations to state that physician-owned hospitals must furnish a list of owners and investors who are physicians or family members at the time a patient requests it. A new rule mandates that a physician-owned hospital require all physicians who are members of the hospital's medical staff to agree, as a condition of continued medical staff membership or admitting privileges, to disclose in writing at the time they refer patients to the hospital any ownership or investment interest in the hospital held by themselves or by an immediate family member. In addition, CMS may terminate a hospital's Medicare provider agreement if it fails to comply with physician ownership requirements.

"Stand in the shoes" provision. CMS has revised the physician "stand in the shoes" provisions to require that only physician owners of a physician organization, and not physicians with an ownership or investment interest that is "titular" only, are deemed to stand in the shoes of that physician organization. An ownership or investment interest is considered "titular" if the physician is not able or entitled to receive any of the financial benefits of ownership or investment.

Entity furnishing DSH. CMS is amending the definition of "entity" to clarify that a person or entity is considered to be "furnishing" designated health services (DHS) if it is the person or entity that has performed the DHS (even if someone else billed the services as DHS) or presented a claim for Medicare benefits for the DHS. If one entity performs a service that is billed by another entity, both entities are DHS entities with respect to that service. The effective date of this change is October 1, 2009, to give affected parties time to restructure arrangements.

Period of disallowance. CMS has placed an outside limit on the period of disallowance during which time a physician can not refer a patient to an entity for the provision of DHS and for which the entity can not bill Medicare because the financial relationship between the referring physician and the entity is not in compliance with all of the requirements of an exception to the general prohibition on physician self-referral.

continued on page 2

Wolters Kluwer Law & Business

Physician self-referral/Stark (cont.)

If the reason for noncompliance does not relate to compensation, the latest the period of disallowance would end, would be the date the arrangement was brought into compliance. If the noncompliance relates to compensation, the period of disallowance ends no later than the date on which all excess compensation is returned to the party that paid it, or on the date on which all additional required compensation is paid to the party to which it is owed.

Signature requirements. If a financial relationship between a health care facility and a referring physician fully complies with Stark provisions regarding financial arrangements between physicians and facilities providing DHS, except for a signature requirement, Medicare payments will be allowed as long as the signature requirement is fulfilled within 90 days, if failure to receive a required signature was inadvertent, or 30 days, if the failure was not inadvertent.

Lease arrangements. CMS has revised the rules to prohibit the use of percentage-based compensation formulae in the determination of rental charges for the lease of office space or equipment. The final rule revises the rules related to lease exceptions, fair market value exception, the exception for indirect compensation arrangements, and provides that per unit-of-service rental charges, also known as "per click" payments, are not allowed to the extent that such charges reflect services provided to patients referred by a physician lessor to the provider lessee. The effective date of these changes is October 1, 2009, to provide affected parties time to restructure arrangements if necessary.

Retirement plans. CMS has clarified that the exclusion from the definition of "ownership or investment interest" related to a retirement plan pertains only to an interest in an entity arising from a retirement plan offered by that entity to the physician (or the physician's immediate family member) through the physician's (or immediate family member's) employment with that entity. CMS made the change because of its concern that some physicians were using retirement plans to purchase or invest in entities other than the one sponsoring the retirement plan to which they refer patients for DHS.

Burden of proof. CMS has clarified that in any appeal of a denial of payment for a DHS that was made on the basis that the service was furnished pursuant to a prohibited referral; the burden of proof is on the provider to establish that the service was not furnished pursuant to a prohibited referral.

Disclosure of financial relationships. CMS plans to send an information collection instrument called a "Disclosure of Financial Relationships Report" (DFRR) to 500 hospitals to help it (1) identify physician arrangements that potentially may not be in compliance with the physician self-referral laws and regulations; and (2) identify practices that may help it in future rulemaking regarding physician self-referral. CMS has "not engaged in a comprehensive reporting initiative to examine financial relationships between hospitals and physicians," since 1991, when it implemented these rules.

The DFRR is a one-time collection effort; however, CMS may use information learned from the collection to issue a notice of proposed rulemaking concerning both the frequency of a future reporting and disclosure process.■

CCH Chicago Bureau, Aug. 8, 2008.

False Claims

Six state false claims acts fall short of DRA requirements

The Office of Inspector General (OIG) issued letters to state officials in Florida, Louisiana, Michigan, New Hampshire, New Mexico and Oklahoma notifying them that their false claims statutes failed to satisfy the requirements of the federal Deficit Reduction Act of 2005 (DRA). Statutes submitted for review by California, Georgia, Indiana and Rhode Island, however, did satisfy the DRA's requirements, making those states eligible for a 10-percent increase in their share of Medicaid false claim recoveries.

The DRA provides a financial incentive for states to enact laws that establish liability for those who submit false or fraudulent claims to the state Medicaid program. States must enact statutes at least as stringent as the federal False Claims Act (FCA) to qualify for the incentive.

continued on page 3

CCH Health Care Compliance Letter

Portfolio Managing Editor
Pamela K. Carron, J.D., LL.M

Coordinating Editors
Susan Smith, J.D., M.A.
Harold Bishop, J.D.
Anthony Nguyen, J.D.

CCH Washington Bureau
Paula Cruickshank
DOJ, FTC–John Scorza
SEC–Peter Feltman
Health Law–Catherine Hubbard, M.A.
Tax–Jeff Carlson, Steve Cooper, Chandra Walker

Designer
Craig Arritola

Requests for information about article submission and comments from readers are welcome and should be directed to Susan Smith at susan.smith@wolterskluwer.com, Tel. 847-267-2780, 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, a Wolters Kluwer business, 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.

False Claims (cont.)

***Qui Tam* problems.** Under the FCA, individuals can bring suit on the government's behalf and retain a portion of any settlement or award the suit yields. In its review letters, OIG determined that the six noncompliant state statutes were not as effective in rewarding and facilitating *qui tam* actions as the federal act. In Louisiana, for example, the state law imposes a shorter statute of limitations on *qui tam* actions than the federal FCA. The New Hampshire false claims act did not meet the DRA requirements because it does not allow a relator to proceed with a *qui tam* action if the state declines to proceed. Under the FCA, a relator may proceed with a *qui tam* action – and collect a percentage of any award – even if the government elects not to join the suit.

Inconsistency. In addition to failing to adequately reward and facilitate *qui tam* actions, the Michigan statute fell short under OIG's review because it does not cover as many instances of Medicaid fraud and abuse as the federal law. The FCA imposes liability against anyone who "knowingly" files a false claim for payment. "Knowingly" is defined broadly under the federal statute, including acts committed in "deliberate ignorance" or "reckless disregard"" of the truth or falsity of information. The Michigan Medicaid False Claim Act does not use the same definition of "knowingly," and thus, does not establish liability for the same range of fraudulent claims.

States that failed to meet the DRA's guidelines were invited to notify OIG if their false claims statutes were amended and to submit them for reconsideration. OIG has previously approved false claims act in eight other states – Hawaii, Illinois, Massachusetts, Nevada, New York, Tennessee, Texas and Virginia. ■

OIG Review Letters, July 24, 2008.

Tax-exempt Organizations

IRS releases updated Form 990 instructions

Updated draft instructions for new Form 990, Return of Organization Exempt from Income Tax, are expected to be posted on the IRS website August 15, 2008. The IRS published revised Form 990 in 2007. The 2008 Form 990 consists of an 11-page core form and 16 schedules. Many of the schedules are new, including: activities outside the U.S., hospitals, tax-exempt bonds, and noncash contributions. Others contain revisions and expansions of existing reporting concerning public charity status and public support, lobbying and political activities, fund-raising and gaming, compensation, transactions with insiders, and related organizations.

The 2008 Form 990 was released without instructions. When the IRS issued draft instructions in April 2008, it identified some common problems with the old instructions. These included no glossary of key terms, unclear definitions, and insufficient guidance in key areas, such as the reporting of activities of disregarded entities and joint ventures owned by the filing organization. The IRS also reported that filers requested more examples in the instructions. The comment period for the draft instructions ended on June 1, 2008.

Key employees. The IRS has revised the definition of "key employee" for purposes of reporting executive compensation, transactions with interested persons, and other items. Under the revised definition, entities will report as key persons only those individuals, other than officers, directors, and trustees, who (1) had reportable compensation exceeding $150,000 for the year; (2) had or shared organization-wide control or influence similar to that of an officer, director, or trustee; or (3) managed or had authority or control over at least 10 percent of the organization's activities (the "responsibility test") and were among the organization's top 20 highest paid persons for the year who satisfied both the $150,000 test and the responsibility test.

Hospitals. Schedule H filers will be required to list in Part V each hospital or other facility that is licensed, registered, or similarly recognized by a state as a health care facility, including facilities other than licensed hospitals. The IRS explained that this does not alter the definition of hospital for purposes of determining whether the organization must complete Schedule H. Addition-

continued on page 7

On The Front Lines

Understanding compliance legal standards in the HIPAA Security Rule, Part I

by John E. Steiner Jr., Esq., Health Care Compliance Advisory Board Member and Brittany Eberle

It is not difficult to find stories about security breaches in which laptops or back-up tapes that contain personal information have been stolen or lost. In some cases, that information has been accessed by people who are not authorized to view it. These breaches are part of the larger world of "security incidents" that fall within the scope of the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA).

Effective compliance programs should include a HIPAA compliance component that encompasses the Privacy Rule as well as the Security Rule. The Privacy Rule addresses what information is protected and how protected health information (PHI) may be used or disclosed.[1]

The Security Rule, which went into effect for most covered entities in April 2005, focuses on what a "covered entity" should implement to protect electronic-PHI (ePHI) that is "created, received, maintained or transmitted" by a covered entity.[2]

Given current capabilities to electronically store and transmit massive amounts of ePHI and the federal government's desire to move toward a national system of digital medical recordkeeping, there is a high priority for the protection of ePHI.[3]

Shortly after the Security Rule went into effect, Providence Health & Services (Providence), located in Seattle, Washington, had several laptops, back-up tapes, and optical disks containing large amounts of ePHI stolen from its facilities. This caught the attention of the press then and again in July 2008, when CMS announced that it had reached a resolution agreement with Providence that requires corrective action on Providence's part. The agreement also requires Providence to pay $100,000 for its possible violations of the Privacy and Security Rules. This marks the first time that HHS has used a resolution agreement as a means of enforcing the Security Rule.[4]

The recent release of the resolution agreement coincides with government plans to audit at least 20 hospitals or health systems in 2008. It is timely for covered entities to renew their familiarity with the compliance legal standards in the statute and regulations. To that end, this article has two main objectives: (1) to summarize major elements of the HIPAA Security Rule and assist in the understanding of applicable compliance legal standards in the rule; and (2) to provide information about Security Rule audits underway by CMS and the Office of Inspector General (OIG). Part I of this article focuses on the legal standards of the Security Rule and Part II will focus on enforcement and sanctions.

Compliance Legal Standards in the Security Rule

Compliance legal standards are set forth in the statutes and regulations that apply to covered entities. Those standards are reflected in specific, affirmative obligations placed on covered entities and in the sanctions provisions.[5]

The statutory requirements for the Security Rule are found in §§1173-1175 of the Social Security Act.[6]

The Security Rule contains four general requirements discussed below and several standards and implementation specifications that a covered entity must meet. A covered entity has a choice of security measures for meeting those requirements. Specifically, security measures chosen by covered entities must be "reasonable and appropriate" to implement the four general requirements and the standards and implementation specifications of the Security Rule. The HIPAA statute and the enforcement regulations set forth the sanctions that can apply if a covered entity fails to meet the requirements. As will be discussed in Part II, sanctions can be levied against covered entities if violations of the Security Rule are due to "willful neglect" rather than "reasonable cause."

Security Rule Requirements

HIPAA requires covered entities to "maintain reasonable and appropriate administrative, technical, and physical safeguards...."[7]

The Security Rule requires that security measures be "reasonable and appropriate" to meet the four general requirements.[8]

These requirements are to:

- ensure the confidentiality, integrity, and availability of all [ePHI] the covered entity creates, receives, maintains, or transmits;
- protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;

- protect against any reasonably anticipated uses or disclosures of [ePHI] that are not permitted or required by the Privacy Rule; and
- ensure compliance with [the Security Rule] by its workforce.[9]

CMS noted that use of the word "ensure" sets a high standard for covered entities; however, no perfectly secure system exists, and should such a system exist, its costs would be prohibitive, especially for smaller covered entities. In the preamble to the final Security Rule, CMS stated that it reads the word "ensure" to require a covered entity to "take steps, to the best of its ability, to protect [ePHI]."[10]

Although the Security Rule does not specify technologies to meet the reasonable and appropriate definition,[11] it requires covered entities to adopt a risk analysis and risk management process that will aid in identifying and addressing security risks. Adhering to such a process, as well as the standards and implementation specifications found in the Security Rule, should help covered entities demonstrate their compliance with the Security Rule.[12]

Security Rule Basics

Safeguards are the actions, measures, policies, procedures, and technology that covered entities implement to protect ePHI. These safeguards are organized into three categories: administrative, physical, and technical. Administrative safeguards protect ePHI through management of the workforce and the "selection, development, implementation and maintenance of security measures." Physical safeguards protect the "information systems and related buildings and equipment" that house ePHI. Technical safeguards "protect [ePHI] and control access to it" through the use of technology. Security measures "encompass all of the administrative, physical, and technical safeguards in an information system."[13]

"… no perfectly secure system exists, and should such a system exist, its costs would be prohibitive, especially for smaller covered entities."

Each category of safeguards in the Security Rule contains "standards" that describe the basic safeguards needed to protect ePHI. Covered entities are required to comply with all the standards in the Security Rule.[14]

Most of the standards are accompanied by "implementation specifications." Implementation specifications give additional detail for the implementation of a standard.[15]

Unlike standards, implementation specifications are either "required" or "addressable." Addressable specifications are not necessarily optional. The Security Rule requires a covered entity to decide whether the addressable implementation specifications are "reasonable and appropriate" given the covered entity's use of ePHI and the vulnerabilities to it. If they are not reasonable and appropriate, then a covered entity must document that decision. If a comparable reasonable and appropriate measure exists, however, it must be implemented in place of an addressable implementation specification.[16]

The standards and implementation specifications of the Security Rule are designed to be "flexible," "scalable," and "technologically neutral," taking into account that covered entities may range from single providers to large health care organizations, which have very different security needs. Therefore, the standards do not require implementation of specific operating systems or hardware.[17]

The flexibility of the standards makes it difficult for covered entities to assess whether by implementing a firewall or encrypting email they have met the requirements of the Security Rule. Again, covered entities must assess whether the security measure used is reasonably or appropriately implementing the standard or specification.[18]

Meeting the Legal Requirements — Risk Analysis and Management

The Security Rule requires covered entities to focus on the process. The first part of the process is in the first two implementation specifications of the Security Rule - conduct a risk analysis and implement risk management. Both implementation specifications are required by the Security Rule and are a foundational piece of a Security Rule compliance program.[19]

A risk analysis is defined as "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability" of the covered entity's ePHI. From the vulnerabilities and threats identified in the risk analysis, the risk management specification requires implementation of security measures that "reduce risks and vulnerabilities to a reasonable and appropriate level to comply" with the four general requirements.[20]

The Security Rule also requires covered entities to consider four additional factors in determining which security measures are appropriate:

- the size, complexity, and capabilities of the covered entity,
- the covered entity's technical infrastructure, hardware, and software security capabilities,
- the costs of security measures, and
- the probability and criticality of potential risks to electronic protected health information.[21]

Meeting the legal requirements — evaluation and maintenance

The final part of this "process oriented" legal standard requires testing the process and continually responding

to new security developments, including new threats and new technologies.[22]

The Security Rule requires this as a separate general rule and as part of the administrative safeguards. The evaluation standard requires covered entities to determine the "extent to which an entity's security policies and procedures meet" the requirements of the Security Rule.[23]

The maintenance general rule requires the review and modification of security measures.[24]

Policies, Procedures and Documentation

The policies, procedures and documentation standards are found outside of the administrative, physical and technical safeguards. Nonetheless, the standards are significant because a covered entity will rely on them to demonstrate compliance with its legal obligations under the Security Rule, especially for investigation or audit purposes. Covered entities must implement policies and procedures that reasonably and appropriately meet the requirements of the Security Rule. Additionally, covered entities must consider the four general requirements in drafting appropriate policies and procedures. The documentation standard requires covered entities to keep their policies and procedures in a written format. In addition, documentation of "action[s], activit[ies] and assessment[s]" must be maintained as required by the Security Rule. Finally, the rule requires covered entities to (1) keep this documentation for at least six years, (2) make it available to those who need it, and (3) periodically revise the documentation.[25]

Conclusion

Part I of this two part article discussed the major requirements of the Security Rule as a framework for a covered entity's assessment of its HIPAA compliance program. Although the rule provides flexibility as to technology, the security measures must be "reasonable and appropriate" to maintain administrative, technical, and physical safeguards. In addition, the rule requires covered entities to adopt a risk analysis and risk management process that will aid in identifying and addressing security risks. Part of that process includes evaluation and maintenance to determine whether the security measures that are in place meet the standards of the rule. Finally, covered entities are required to maintain and implement policies and procedures. Written documentation of policies and procedures as well as actions, activities and assessments will help demonstrate compliance with the Security Rule should CMS or OIG conduct an audit or investigation of the entity. Part II will focus on sanctions, audits and enforcement policies under the Security Rule. ■

John E. Steiner Jr., Esq., CHC is the Chief Compliance Officer for UK Health Care of the University of Kentucky of Lexington, Kentucky. He previously served as Chief Compliance Officer and Privacy Officer for the Cleveland Clinic, as Senior Counsel for the American Hospital Association, and as a member of the health law department of a national law firm. He is a member of the CCH Health Care Compliance Editorial Advisory Board.

Brittany Eberle is a third year law student at the University of Kentucky. She is expected to graduate in May 2009.

1 See generally HIPAA Privacy Rule, 45 C.F.R. Part 160, Part 164 Subparts A & E; see *also* Final rule, 68 FR 8335, February 20, 2003.

2 See *generally* 45 C.F.R. Part 160, Part 164 Subparts A & E.; Final rule *supra* note 1. A "covered entity" is either a "health plan," a "health care clearinghouse," or a "health care provider who transmits any health information in electronic form in connection with a transaction covered" by HIPAA. 45 C.F.R. §§ 160.103, 164.318.

3 See CMS, Security 101 for Covered Entities, 4 (2007) *available at* http://www.cms.hhs.gov/EducationMaterials/Downloads/Security101forCoveredEntities.pdf.

4 *HHS, Providence Health Services Agree on Corrective Action Plan to Protect Health Information*, (July 17, 2008) *available at* http://www.hhs.gov/ocr/privacy/enforcement/resolution.html.

5 John Steiner, *Understanding compliance legal standards as a key element in a compliance program, Health Care Compliance Letter*, Vol. 11, Issue 7, April 1, 2008.

6 See Health Insurance Portability and Accountability Act of 1996 (PubLNo 104-191) as codified in 42 U.S.C. §§ 1320d-2 - d-4.

7 Social Security Act §1173(d)(2).

8 See 45 C.F.R. §§ 164.306(a)-(b)(1), 164.308(a)(1)(ii)(B); Final rule, *supra* note 1, at 8341.

9 45 C.F.R. § 164.306(a)(1)-(4).

10 Final rule *supra* note 1, at 8346.

11 CMS, *Security 101 for Covered Entities*, *supra* note 3, at 8.

12 See Thomas J. Smedinghoff, *It's All About Trust: Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law*, 16 Mich. St. J. Int'l L. 1, 29-37 (2007).

13 Social Security Act §1173(d)(2)); 45 C.F.R. §§ 164.304, 164.308,164.310; 164.312.

14 45 C.F.R. § 164.306(c).

15 45 C.F.R. § 160.103.

16 45 C.F.R. § 164.306(d); CMS, *Security 101 for Covered Entities*, *supra* note 3, at 5-6.

17 45 C.F.R. § 164.306(b); CMS, *Security 101 for Covered Entities*, *supra* note 3, at 7-8.

18 45 C.F.R. § 164.306(b).

19 45 C.F.R. § 164.308(a)(ii)(A)-(B); Final rule, *supra* note 1, at 8346; CMS, *Basics of Risk Analysis and Risk Management*, 2 (2007), *available at* http://www.cms.hhs.gov/EducationMaterials/Downloads/BasicsofRiskAnalysisandRiskManagement.pdf; see also Smedinghoff, *supra* note 12, at 32-38.

20 45 C.F.R. § 164.308(a)(1)(ii)(A)-(B).

21 45 C.F.R. § 164.306(b)(2)(i)-(iv).

22 Smedinghoff, *supra* note 12, at 34; CMS, *Basics of Risk Analysis and Risk Management*, *supra* note 19, at 15-16.

23 45 C.F.R. § 164.308(a)(8).

24 45 C.F.R. § 164.306(e).

25 45 C.F.R. § 164.316(a)-(b)(1)-(2).

ally, physician clinics and skilled nursing facilities will be eligible for treatment as subsidized health services in accordance with the generally applicable rules regarding subsidized health services.

Form 990-EZ concerns. The draft instructions require a controlling organization to file Form 990, rather than Form 990-EZ, if it (1) controls one or more controlled entities within the meaning of IRS Code §512(b)(13), and if (2) there was any transfer of funds between the controlling organization and any controlled entity during the year, the American Institute of Certified Public Accountants (AICPA) told CCH. This requirement, the AICPA noted, will be burdensome on small organizations, such as trade associations, that have an affiliated Code §501(c)(3) foundation or other tax-exempt affiliate meeting the definition of a controlled entity, as they otherwise would be permitted to file Form 990-EZ during the Form 990 transition period. The AICPA recommended that small controlling organizations with tax-exempt controlled entities be allowed to file Form 990-EZ, assuming there are no unrelated business income tax issues, along with filing Form 990, Schedule R. ■

CCH Washington Bureau, Aug. 6, 2008.

HIPAA

Information security breaches growing in health care

Security breaches in the health care industry have become more widespread and are affecting all segments of the industry, including health insurers, hospitals, pharmacies, physicians and vendors. During a recent American Bar Association teleconference, attorney Melissa Markey, of Hall, Render, Killian, Heath and Lyman, noted that according to the Identity Theft Resource Center, in the first half of 2008, there were 56 reported breaches of health care information that exposed almost three million records, amounting to nearly 15 percent of all reported data breaches.

Kirk Nahra, a partner with Wiley Rein & Fielding, warned that identity theft is a major driving force in many of today's most significant developments, motivating regulators and enforcement agencies because of actual, identifiable harms. He stressed "the enforcement world is changing. Changes are incremental, but we are learning more about what the government wants and expects," adding that this gives health care companies lots of opportunities for self-evaluation.

Risk assessment. Nahra suggested that organizations conduct a new risk assessment if they have not done so for a while."If you haven't updated recently, you aren't doing a good enough job," he stated, adding that every significant change to the computer environment may cause a shift in the hazards and vulnerabilities of systems. Markey added that it's a good time to prepare for e-discovery compliance and evaluate document management policies and acceptable use policies." If you're letting your doctor's use [instant messaging] for patient information, this might be a really good time to think about how you're protecting that information in transit and how you're getting that information in your electronic medical record," she noted.

HIPAA rules. According to Markey and Nahra, entities covered under the Health Insurance Portability and Accountability Act (HIPAA) must: (1) conduct a risk analysis and use that as a basis for risk management strategies; (2) develop and implement physical, technical and administrative safeguards; (3) enforce their sanctions policies; and (4) respond to security incidents. "The regulators will react extremely badly if you have a sanction policy, but you do not enforce it against a physician who inappropriately allows his office staff to access private health information (PHI) that they don't need to see," Markey cautioned. (See On the Front Lines on page 4 for a detailed discussion of compliance with the HIPAA Security Rule.)

The HIPAA Security Rule describes an appropriate "process" that covered entities must go through in evaluating security options, broken down into technical, physical and administrative safeguards, Nahra noted. According to Nahra, the two most important parts of that process are: (1) risk analysis, conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity; and (2) risk management, which involves an obligation to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Mitigation. Nahra noted that mitigation is an important piece of HIPAA compliance. Mitigation involves: (1) identifying the problem; (2) determining the cause of the problem; (3) evaluating any potential risks; and (4) "stopping the bleeding" from the problem, for example, shutting down a system that is helping to cause the breach to occur. "You need to fix the problem and make sure it doesn't happen again," he said.

Other key issues to consider include what data is involved, whether it was encrypted, whether the data was electronic or paper (or something else), what states are involved, the likelihood of harm, consumer attitudes, and actions required by law, Nahra added. He explained that in some cases the entity may choose to notify patients or customers even when it's not required by law.

Security enforcement. CMS has hired PriceWaterhouseCoopers to assist them in the development and execution of HIPAA security audits. In addition, CMS announced that it will conduct about 20 assessments in 2008 and that onsite investigations "may be triggered by complaints alleging noncompliance," Markey stated. State attorneys general, the Federal Trade Commission and Insurance Commissioners may be a more significant threat, Nahra added. ■

CCH Washington Bureau, July 31, 2008.

Medicare

CMS expands number of "never events" in IPPS final rule

CMS has expanded the number of preventable conditions for which it will not pay inpatient hospitals as part of the final rule for the inpatient hospital prospective payment system (IPPS) for fiscal year (FY) 2009. The list of so-called "never events" are preventable medical errors that result in serious consequences for the patient.

In the FY 2008 IPPS update, CMS listed eight preventable hospital-acquired conditions (HACs) for which it would not make additional payments. The final rule includes three additional HACs: (1) surgical site infections following certain elective procedures, including certain orthopedic surgeries, and bariatric surgery for obesity; (2) certain manifestations of poor control of blood sugar levels; and (3) deep vein thrombosis or pulmonary embolism following total knee and hip replacement procedures. CMS has sent a letter to state Medicaid directors encouraging states to adopt the same no payment policy regarding never events.

The final rule also expands the Reporting Hospital Quality Data for Annual Payment Update program. Hospitals currently are required to report 30 quality measures on Medicare claims to qualify for the full market basket update. The final rule includes 13 new measures. One measure—oxygenation assessment—will be retired, so hospitals will be required to report on 42 measures in FY 2009.

Apart from the final rule, CMS announced a process to develop three National Coverage Determinations (NCDs) to address Medicare coverage of the following surgical procedures: (1) surgery on the wrong body part; (2) surgery on the wrong patient; and (3) the wrong surgery performed on a patient. CMS began accepting comments from the public regarding these NCDs on July 31, 2008, for a 30-day period. A proposed decision memorandum will be released on or before February 1, 2009, for public comments and finalized no later than April 30, 2009. ■

Advance release of Final rule, Aug. 1, 2008.

In the News

DOJ announces settlement with Cox Medical Centers

The U.S. Attorney for the Western District of Missouri has entered into a $60 million settlement with the Lester E. Cox Medical Centers to resolve allegations of violations of the physician self-referral prohibition, the anti-kickback statute, and the False Claims Act (FCA). The allegations include: (1) Cox entered into prohibited financial arrangements with a physician group to induce physicians to refer patients to Cox, in violation of the Stark law and the anti-kickback statute; (2) Cox submitted Medicare cost reports that employed an improper method of reporting its medical clinics' overhead that resulted in fraudulent claims for nonreimbursable clinic costs; and (3) through entities controlled by Cox, Cox improperly billed for end stage renal disease treatments provided to patients in violation of the FCA. The settlement amount, which is considerably less than the alleged improper Medicare payments, took into account Cox's ability to pay and to continue providing medical care to the community.

DOJ News Release, July 22, 2008.

HRSA awards $12 million for nursing faculty and diversity

The Health Resources and Services Administration (HRSA) announced $12 million in grants to further the education and training of the nation's nurses and nursing educators, and increase diversity in nursing. Twenty-eight new "Nurse Education Practice and Retention Program" grants worth $8.5 million were awarded to 25 academic institutions and three hospital organizations to address the nursing shortage by strengthening capacity for nurse education, practice, and retention. These grants support partnerships among collegiate schools of nursing, academic health centers, accredited public or private institutions and other organizations. Nine new "Nursing Workforce Diversity Program" awards totaling $2.8 million were made to seven universities and two community colleges to help educate and support pre-nursing and nursing students from disadvantaged backgrounds, including racial and ethnic minorities.

HRSA News Release, Aug. 1, 2008.

Medicare has a role in overall health care reform

Policymakers should not separate Medicare reform from reform of overall health care system, according to the Center on Budget and Policy Priorities (CBPP). CBPP reports that changes to Medicare, if properly designed, can complement system-wide health care reform and the two should be pursued simultaneously. Medicare, as the largest U.S. purchaser and regulator of health care, exerts a major influence on the rest of the health care system and can play an important role in slowing the growth of both public and private health care costs. Policymakers should seek out initiatives that have the potential to strengthen Medicare's financial status and, serve as a model for the rest of the health care system. CBPP believes that lawmakers could: (1) eliminate the overpayments that Medicare is making to insurance companies that participate in Medicare Advantage; (2) establish a vigorous research program on the comparative effectiveness of different health care treatments and procedures; (3) alter Medicare's payment systems to reward improved quality and efficiency; (4) promote the use of electronic health records as a means of improving communication, decreasing unnecessary services, and controlling fraud; and (5) require physicians participating in Medicare to issue prescriptions electronically.

CBPP Report, July 31, 2008