CCH Health Care Compliance LETTER

Volume 8, Issue 14 health.cch.com July 11, 2005

Submission of Articles. Requests for information about article submission guidelines should be sent directly to Andra Popa at popaa@cch.com.

Comments? Please direct any questions or comments regarding articles appearing in the newsletter to the e-mail address above.

For more information about the CCH Health Care Compliance Portfolio, please visit our online store at http://health.cch.com.

Ensuring an accurate and efficient billing process

by Catherine Hubbard, M.A., Contributing Editor

To make sure the patient accounting billing process of a health care organization is running efficiently, while maintaining data integrity, compliance officers and executives must pay special attention to monitoring, auditing, educating and preventing billing errors.

One way to develop a plan for compliance auditing and monitoring is to follow the seven-component framework developed by the Association of Healthcare Internal Auditors and the Health Care Compliance Association.

Risk assessment. First, health care organizations should conduct a thorough risk assessment, according to Debi Weatherford, vice president of compliance and audit services at Revenue Cycle Solutions, located in Pittsburgh, Pa. "It is important for each organization to customize an audit based on the organization's risk," she said during a recent Healthcare Financial Management Association audio conference.

Understand laws and regulations. "The laws of a year ago may not be the laws of today," she said. "On any specific issue, as you look at the issue from a compliance auditing and monitoring standpoint, it is important to understand the existing laws and their interpretation."

Establish policies. Health care organizations should obtain and establish policies for specific issues and areas, Weatherford said, stressing the importance of developing policies that address key risk areas for the organization. Policies should be reviewed and updated periodically, she added.

Educate and re-educate staff. In addition, educating employees as to policies and procedures and communicating awareness "is critical at each level of the organization," said Weatherford. Various levels of employees should be aware of auditing and monitoring issues and how the organization is addressing them, she stressed. She added that organizations need to educate and re-educate staff on regulations and issues identified through auditing and monitoring efforts.

Finally, Weatherford emphasized that organizations need to document their auditing and monitoring processes. "If your organization should ever get into trouble on an issue, it is very important that you maintain the documentation that supports your efforts, which can help mitigate some damages."

Audit and monitor compliance. Mark Ruppert, director of internal audit at Cedars-Sinai Health System in Los Angeles, explained that a formal audit is governed by professional standards and completed by professionals independent of the health care organization. Rupert highlighted several key components: planning, identifying risk areas, assessing internal controls, sampling of data, testing of processes, and validating information. "This requires a more methodical and structured approach," he added.

Corrective actions should be communicated formally with both management and the Board, Ruppert said, adding that communications also should include a document follow-up of corrective actions. "The follow-up will determine if the recommended corrective actions were actually put into place," he said

Usually, departmental staff communicates with management through formal communications to operations leaders and not necessarily to the Board, Ruppert said. "It is very important to create a collaboration between the auditor or the monitors and legal and compliance," he said. "You really want to coordinate with your compliance officer and general counsel, because of the reporting requirements that may come from what you find," he added.

Outlier payments. Ruppert demonstrated how the seven-component framework can be applied in two areas: outlier payments and charity care. He noted that organizations do not need to apply the components in a given order, but can apply the components as appropriate.

Policies and procedures. The first step relative to outliers is to determine the history and extent of outlier payments and related denials at the organization, initially through discussions with patient financial services and finance, Ruppert outlined. "One thing you are looking for is [whether there has] been rapid increases in your gross charges or outlier reimbursements," he said.

When developing policies and procedures, it is important to remember that policies regarding outlier payments do not need to be specific, said Ruppert. "You may not have an outlier payment policy, but you may have billing policies and you want to determine if those policies address the key outlier issues," he said. He also advised that organizations analyze policies related to control over the charge description master (CDM) to make sure that gross charges are not arbitrarily changed.

Regarding the monitoring component, Ruppert said organizations should apply the fiscal intermediary's audit approach, if one is available, to routine sampling on a monthly, quarterly or semi-annual basis, depending on the organization's risk and resources.

Auditing. For auditing, the organization should assess the adequacy of controls over CDM charges and updates, select a random sample of inpatient and outpatient accounts, complete a line item review of CDM charges on the patient bill and then verify the appropriateness and medical necessity of each. The organization should also ensure accuracy of billable units, he said. "A dose is not always a dose, depending on how it is billed," Ruppert stated.

Charity care. Ruppert also told the audience how to apply the components of an audit to charity care, which is generally a concern of tax-exempt hospitals and hospital systems. During the risk assessment phase, the tax-exempt hospital or hospital system should assess the following:

- whether the organization has a charity care mission;
- whether specific charitable care policies are in place;
- whether the charitable care policies are uniform across all units and clinics;
- whether patients are informed of the charitable care policies;
- whether the attorney general is targeting the issue in its state.

Furthermore, tax-exempt hospitals and hospital systems should be familiar with the Internal Revenue Service's (IRS's) enforcement initiative against non-profit entities. In addition, the tax-exempt hospitals and hospital systems should also determine the minimum amount of charity care necessary for the entity to maintain tax-exempt status, if any, and should review related state and local regulations that define charitable care.

When analyzing policies and procedures, organizations should make sure charity care guidelines define billing and collection practices. Policies should address the actions of collection agencies, he said. "In most cases, you are going to have collection agencies doing [the work] and they need to be applying the same criteria that your own billing staff would use in charity care situations," he advised.

Monitoring conversion of bad debt to charity care should occur on a monthly basis, said Ruppert. "Pursue any noticeable increases," he advised. Organizations also should review self-pay conversion to Medicaid or other programs, confirm application of their billing and collections policy consistently across units, and analyze collector activity to determine whether collectors are complying with the organization's policies.

During the audit process, the organization needs to ensure that its policy and definition of charity care is consistent with related laws and across units, to verify charitable care calculations completed by external auditors, and to verify that charitable care reported on its financial statement meets its own charity care write-offs, Ruppert said.

CCH Health Care Compliance Letter

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

Coordinating Editors
Susan Smith, J.D., M.A.
Andra Popa, J.D., LL.M

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

Designer
Kaveh D. Ryndak

Comments from readers are welcome and should be directed to Andra Popa at popaa@cch.com, Tel. 847-267-2476, 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.

In addition, the organization should identify the charity care write-off transaction codes used in its billing system and select a sample of write-offs. "Select that sample across all units and clinics so that you get a good feel for application and policy," Ruppert said.

Billing. When monitoring and auditing the pre-billing process, organizations should examine their performance reporting for transcription completion. "You want to always be in the loop," Weatherford said. Organizations should develop reports to identify and correct data before the claim is billed, she added.

To make sure the pre-billing process is working smoothly, organizations should match certifications to charges and should confirm the number of days authorized for each level of care, the hours authorized for observation, and the therapy treatments authorized, said Weatherford.

It is also important to review how the organization tracks and reviews late charges and changes to charges, she said. "Whatever process you have in place, you want to make sure there are checks and balances to make sure that the person who made the change understood the charge," she said.

The organization will want to identify accounts for potential interim billing and consolidate billing when possible, Weatherford added. "In the billing process, you want to make sure that whatever you see will help streamline the process for a claim to go through your system and that you identify any points where claims get bogged down in your process," Weatherford said.

Developing automated methods for cash payments, credit balance reports and record requests can not only streamline the process, but also increase accuracy. "There should be an automated system," she concluded.

CCH Washington Bureau, July 11, 2005

Proposed rule: New contractors for Medicare program integrity

by Sheila Lynch-Afryl, J.D., Contributing Editor

Proposed regulations implementing the Medicare Integrity Program (MIP), which was established by the Health Insurance Portability and Accountability Act of 1996 (PubLNo 104-191), would amend 42 C.F.R. Part 421 by adding a new subpart D. In addition, proposed regulations concerning contracts with fiscal intermediaries and carriers would bring current regulations into conformity with the Social Security Act.

Medicare program integrity contractors. Under the new subpart D entitled "Medicare Program Integrity Contractors," a MIP contractor would be defined as an entity that has a contract with CMS to perform exclusively one or more of the program integrity activities specified in Soc. Sec. Act § 1893. The following would be considered MIP activities: (1) medical, utilization, and fraud review, (2) cost report audits, (3) Medicare Secondary Payer activities, (4) education, and (5) developing prior authorization lists of durable medical equipment. MIP functions would apply to all types of claims and all payment systems, including payment under Part D, the outpatient drug benefit beginning January 1, 2006.

Eligibility. An entity would be eligible to enter into a MIP contract if it demonstrates the capability to perform MIP contractor functions; agrees to cooperate with the Office of Inspector General and the Department of Justice in the investigation and deterrence of potential fraud and abuse in the Medicare program; and complies with the conflict of interest standards. It also must maintain a written code of conduct and compliance policies that include a policy on employee conflicts of interest and meet financial and business integrity requirements.

Conflict of interest. CMS will not enter into a MIP contract with a contractor that has, or has the potential for, an unresolved organizational conflict of interest. If CMS discovers a conflict of interest during the term of the contract, CMS may elect to modify, terminate, or not renew the contract.

Under the proposed rule, a Medicare Administrative Contractor (MAC), as well as fiscal intermediaries and carriers that had a contract with CMS on August 21, 1996, would be allowed to perform any or all of the MIP functions until fiscal intermediaries and carriers are phased out in September 2011 in accordance with §911(d) of the Medicare Modernization Act (PubLNo 108-173) (MMA). While they may not duplicate work being performed under a MIP contract, they may develop and update a list of items of durable medical equipment that are subject to prior authorization.

CMS would award contracts in accordance with acquisition regulations set forth at 48 C.F.R. chapters 1 and 3. The regulations would specify that CMS may renew a MIP contract without competition if the contractor continues to meet all the requirements of proposed subpart D and meets the performance standards and requirements of the contract.

continued on page 8

National electronic health record implementation picks up speed through federal leadership and public/private sector cooperation

by Aggie Stewart, M.A.

Although an increasing number of individual healthcare organizations have forged ahead with the development and use of some form of an electronic health record, nationwide implementation of a fully realized, interoperative electronic health record has moved along at a much slower pace. Interoperative information or interoperability refers to "the ability to exchange patient health information among disparate clinicians and other authorized entities in real time and under stringent security, privacy and other protections."[1] *Pressure to pick up the pace has come from many quarters, not least of which came in response to two reports published by the Institute of Medicine entitled* To Err is Human: Building a Safer Health System (2000) *and* Crossing the Quality Chasm: A New Health System for the 21st Century (2001). *The greatest impetus to increase the pace of activity, however, has and continues to come from the federal government, which, as a payor of more than one third of all healthcare costs, remains one of the largest stakeholders in healthcare.*

Today, an unprecedented amount of public/private sector activity—coordinated under federal leadership within the Department of Health and Human Services (HHS)—is occurring toward creating a national health information network to support widespread health information exchange and an interoperable electronic health record. The pace and comprehensive nature of this activity has grown largely out of the federal government's recognition that the multitude of competitive interests in the healthcare marketplace has prevented a unified effort to achieve common standards and interoperability. The Office of the National Coordinator for Health Information Technology in HHS and the post of the National Coordinator were established last year to ensure that public and private sector efforts were aligned and mutually supportive of common goals. Federal involvement at this level is the result of initiatives begun in the 1990s to capitalize on the benefits of evolving information technology.

Roots of federal involvement. The federal government's involvement reaches back to 1993 when former President Clinton established the Information Infrastructure Initiative, which included a Health Information and Applications Workgroup. The National Committee on Vital and Health Statistics, the public advisory body for the Secretary of HHS on national health information policy, recognized the opportunities and interest in integrated health information strategies, particularly in light of the health data mandates stemming from the Health Insurance Portability and Accountability Act (HIPAA) legislation.

In 1998, the National Committee on Vital and Health Statistics convened another workgroup, this time devoted to the creation of a National Health Information Infrastructure. The workgroup, a public-private sector effort, launched an 18 month review of current and emerging health information systems that included hearings and consultations with healthcare providers, public health professionals, consumer representatives, and healthcare information technology representatives. The National Committee on Vital and Health Statistics published the findings of this review in its November 2001 report and recommendations to HHS in a report entitled *Information for Health: A Strategy for Building the National Health Information Infrastructure* (*Information for Health*). This ground-breaking work established a working definition of such an infrastructure, one that encompassed the technologies, standards, applications, systems, values, and laws that could support all facets of individual health, healthcare, and public health. In addition to enabling the delivery of health and health-related information where and when it is needed, the goals of the National Health Information Infrastructure included devising a system that would improve and enhance the security, privacy, and confidentiality of personal health information (PHI). The National Health Information Infrastructure's work continued at interim meet-

ings and two summer conferences in 2003 and 2004. These forums brought together representatives from the public and private sectors of the healthcare industry in unprecedented numbers for working sessions in which critical components of the National Health Information Infrastructure, such as architecture, standards and vocabulary, and privacy and confidentiality, were developed.

Momentum increases under federal leadership. *Information for Health* increased substantially the momentum behind creating a national, interoperable health information network. Through the public hearings that were a part of the 18-month review that provided the foundation for the report, the National Committee on Vital and Health Statistics "determined that the most important missing ingredient, which could accelerate and coordinate progress on the National Health Information Infrastructure, is leadership, specifically, federal leadership."[2] In response, it recommended that:

> a new senior position and office at the U.S. Department of Health and Human Services (equipped with adequate funding) be developed to oversee and coordinate a broad range of health information policy, research, and program activities in different sectors, both public and private. This office should have the resources and mandate to coordinate all efforts for the National Health Information Infrastructure, internally and externally and in both public and private sectors, and to directly fund strategic cross-cutting activities. The new office should exercise both horizontal and vertical coordination: horizontally, across healthcare providers, consumers, public health programs, standards development organizations, payers, government agencies, academic and healthcare institutions, and others, and vertically, through local, State, and national entities. It must explicitly encompass the personal health, healthcare provider, and population health dimensions rather than focus on any single area. At the same time, the National Health Information Infrastructure-related activities of each HHS agency need to be strengthened and new resources added under the general coordination of the new office.[3]

In April 2004, President Bush created The Office of the National Coordinator for Health Information Technology and in May appointed the first-ever National Health Information Technology Coordinator, David J. Brailer, MD, PhD, to provide the necessary leadership to create an electronic health record within a decade. The Office of the National Coordinator is responsible for directing federal initiatives relating to health information technology. This involves activities and projects across 15 federal agencies and organizations, listed below:

- Assistant Secretary for Planning and Evaluation
- Office of the National Coordinator for Health Information Technology
- Council on the Application of Health Information Technology
- Agency for Healthcare Research and Quality
- Centers for Medicare and Medicaid Services
- Food and Drug Administration
- National Institutes of Health
- Indian Health Service
- Health Service and Resource Administration
- Centers for Disease Control and Prevention
- Department of Commerce
- Department of Defense/ Veterans Affairs Initiatives
- Department of Veteran Affairs Initiatives
- Department of Homeland Security

The decade of health information technology. By July 2004, Dr. Brailer had prepared and issued the outline of a plan to build the national health information infrastructure within 10 years. The plan was included in the report The Decade of Health Information Technology: Delivering Consumer-Centric, Information-Rich Health Care and identified four major goals and 12 corresponding strategies for focusing and advancing efforts to achieve an interoperable electronic health record with joint public/private cooperation and leadership:

Inform clinical practice

(1) Incentivize electronic health record adoption
(2) Reduce risk of electronic health record adoption investment
(3) Promote electronic health record diffusion in rural and underserved areas

Interconnect clinicians

(1) Foster regional collaborations
(2) Develop a national health information network
(3) Coordinate federal health information systems

Personalize care

(1) Encourage use of personal health records
(2) Enhance informed consumer choice
(3) Promote use of telehealth systems

Improve population health[4]

(1) Unify public health surveillance architectures
(2) Streamline quality and health status monitoring
(3) Accelerate research and dissemination of evidence

Achieving these goals will require a level of interoperability—supported by compliance with HIPAA regulations—that poses one of the greatest challenges to this entire undertaking.

Continuing to reach out for ideas. In order to gain broad input on how best to achieve nationwide interoperability, HHS published a request for information (RFI) last November, seeking input on the development and adoption

of a national health information network. HHS intends to use the information from responses to inform policy discussions about possible methods by which widespread interoperability and health information exchange could be deployed and operated on a sustainable basis. The RFI asked 24 questions across six categories:

- General information
- Organizational and business framework
- Management and operational considerations
- Standards and policies to achieve interoperability
- Financial and/or regulatory incentives and
- Legal considerations and other considerations, including design principles and measures of success

In early June, HHS released its report Summary of Nationwide Health Information Network Request for Information (RFI) Responses, which presents an overview of the more than 500 responses it received from organizations and individuals about how to move forward. While the report provides a synopsis of responses, it does not attempt to evaluate or discuss the relative merits of any one response over another. Nonetheless, it does provide some key findings. Among the many opinions expressed, significant support emerged for the following concepts:

- A national health information network should be a decentralized architecture built using the Internet, linked by uniform communications and a software framework of open standards and policies.
- A national health information network should reflect the interests of all stakeholders and be a joint public/private effort.
- A governance entity composed of public and private stakeholders should oversee the determination of standards and policies.
- A national health information network should be patient-centric with sufficient safeguards to protect the privacy of personal health information (PHI).
- Incentives will be needed to accelerate the deployment and adoption of a national health information network.
- Existing technologies, federal leadership, prototype regional exchange efforts, and certification of electronic health records will be the critical enablers of a national health information network.

Respondents identified key challenges to developing and adopting a national health information network, including:

- the need for additional and more refined standards;
- addressing privacy concerns;
- paying for the development and operation of, and access to, the national health information network;
- accurately matching patients identity; and
- addressing discordant inter- and intra-state laws regarding health information exchange.

According to HHS, nearly every RFI response addressed the issue of patient privacy. One of the key principles that emerged from these comments was that privacy and security should be viewed as fundamental business and technical requirements of a national health information network with respect to the development of its architecture, data access and control policies, business rules and governance models. Use of a national patient identifier in a national health information network turned up as a leading privacy concern. Respondents felt that the risk of accidental and intentional privacy and security breaches would be heightened through its use.

HHS noted other major privacy considerations from the RFI respondents, including:

- Health record ownership. There is currently little agreement regarding who owns or should own the patient health record (e.g., the patient, various providers, health plan), who maintains it, what constitutes it, and which medical providers or payers should have access to the record in whole or in part.
- Consumer opt-in versus opt-out model for national health information network adoption. This refers to whether the patient would have to actively consent to having his or her information available via a national health information network. Under the opt-in model, the volume of records available would grow much more slowly as patients learned about a national health information network and decided whether or not to participate. The opt-out model would require less overhead, but could lead to patients' perceptions that their information was shared without their consent.
- Disclosure limitations and whether new limitations on the disclosure of health information.
- Role-based user access features. Role-based access mechanisms allow patients to grant permission to classes of providers at a given institution to view certain portions of their records while screening information from other users. According to HHS, the most frequently cited example of this was a feature to shield mental health-related information from all users except certain mental health professionals.
- User authentication. The HHS report shows that a number of respondents identify authentication of national health information network users (e.g., physicians, providers, payer staff, researchers, patients themselves) as an important national health information network security element. It was often recommended that various forms of authorization be required before a user could view, change, or add data to specific patient records.
- Consumer education. The HHS report also shows support for public awareness campaigns to educate consumers about privacy considerations regarding their national health information network participation rights and the benefits of health information exchange.
- De-identified data. There seemed to be general agreement on the usefulness of de-identified patient data for bio-surveillance, public health, and clinical research.

More than half the responses to the RFI came from individuals, including physicians and private citizens. According to HHS, these respondents tended to make general statements about the national health information network concept without addressing the specific RFI questions and expressed a great deal of worry

over privacy and security. Concerns ranged from opposition to the creation of federal or state government databases, to the need for an informed consent requirement for participation, to significant reservations about the ability to maintain appropriate patient confidentiality within any type of national health information network model. Unauthorized access to patient records surfaced as a primary scenario these respondents wanted to avoid. Overall, this group expressed significant reservation and often direct opposition to a national health information network.

Next Steps. HHS has begun the next phase of its health information technology (HIT) strategy by issuing four requests for proposals (RFPs) which address some of the key challenges identified in its summary of national health information network RFI responses.

- **Standards.** Currently, there are many standards for information exchange, clinical vocabulary, and coding, but they lack integration with each other. Moreover, there are gaps in the standards. This situation may hinder interoperability and widespread adoption of HIT. In this RFP, HHS is looking for a contractor to develop, prototype, and evaluate a "harmonization" process for achieving a widely accepted and useful set of standards that will enable and support interoperability among healthcare software applications, particularly electronic health records.
- **Certification.** With more than 200 electronic health record products on the market today, there are no criteria to evaluate product functionality and interoperability. Having such criteria would reduce the risk of HIT investment and contribute to making more informed purchasing decisions by health care providers. In this RFP, HHS is looking for a contractor to develop criteria that address electronic health record functionality and include ambulatory and inpatient features, decision support features, and performance reporting. The criteria must also include interoperability, security, and reliability features. Interoperability features will be based on the national health information network prototypes created through the RFP below.
- **Prototypes for a national health information network architecture.** Currently, there is no consensus on how to use the available Internet infrastructure to support interoperable health information exchange. In this RFP, HHS is looking to develop and evaluate prototypes for an Internet-based national health information network architecture that would maximize the use of existing resources, such as the Internet, to achieve widespread interoperability among healthcare software applications, particularly electronic health records. A key objective of this RPF is to spur technical innovation for nationwide sharing of health information in patient care and public health settings. Up to six contracts will be awarded. Contractors must demonstrate interoperable health information exchange in real-world healthcare environments, maximizing the use of existing infrastructure.
- **Privacy and security solutions for health information exchange.** Currently, providers implement required security and privacy business policies in a variety of ways tailored to individual organizations, presenting challenges to widespread electronic information exchange (e.g., one hospital may use a password while another uses a biometric fingerprint for security). In this RFP, HHS is looking to assess and develop solutions to address state and business privacy and security practices that may pose challenges to implementing an interoperable health information exchange. The contractor will work in direct collaboration with states or territories to engage public and private sector healthcare stakeholders involved in interoperable health information exchange. The contractor will develop and execute a plan to assess and analyse the impact of business policies and state laws on security and privacy practices and to develop solutions. The analysis will result in identifying and documenting best practices, lessons learned, and solutions used to address variations in privacy and security practices. Finally, the contractor will ensure consensus and will hold one or more national meetings to synthesize findings to help develop the national health information network prototype and to inform federal, state, and local policy.

Realizing the Vision. Considerable progress is being made towards implementing a fully realized, interoperable electronic health record within a national health information network. Under the leadership provided by HHS and the Office of the National Coordinator for Health Information Technology, the public and private sectors within healthcare are working together effectively to transform healthcare through the application of HIT. While we are still some distance from achieving the goal of what is arguably one of the most complex transformations the industry has experienced, lessons learned from recent large-scale implementations, such as the HIPAA regulations, must be a touchstone to help navigate some of the more challenging issues to be sorted out and resolved, particularly integrated standards, privacy, and security.

[1] Department of Health and Human Services, National Coordinator for Health Information Technology. Development and Adoption of a National Health Information Network. November 15, 2004.

[2] NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS. *Information for Health: A Strategy for Building the National Health Information Infrastructure.* Washington, DC. November 2001, p 3. This report is available on the Internet: http://aspe.hhs.gov/sp/National Health Information Infrastructure/Documents/National Health Information Infrastructurelayo.pdf.

[3] NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS. *Information for Health: A Strategy for Building the National Health Information Infrastructure.* Washington, DC. November 2001, pp 3-4.

[4] Thompson, Tommy G. and Brailer, David J. MD, PhD. *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care, Framework for Strategic Action*, Washington, DC. July 2004, pp b-c. This report is available on the Internet: http://www.hhs.gov/healthit/documents/hitframework.pdf.

Aggie Stewart, M.A., is a healthcare freelance writer. She publishes on a range of subjects related to health information management and technology, particularly electronic health records, as well as healthcare quality and compliance. She recently published Understanding Reimbursement to Small and Rural Hospitals (CCH, Inc., 2005) and was Consulting Editor of Health Information Management Manual, second edition (Aspen Publishers, 2002), a comprehensive anthology of print and electronic resources for health information management and technology leaders.

Fraud & Abuse (cont.)

Intermediaries and carriers. Currently, CMS contracts with fiscal intermediaries for the administration of Part A and with carriers for the administration of Part B. Section 911 of the MMA eliminated the requirement that intermediaries be nominated and establishes the requirement that contracts awarded to MACs be competitively bid. Between 2005 and 2011, CMS will conduct competitions to replace the current contracts with MACs.

Proposed regulations also would distinguish between those functions that the Act requires to be included in agreements with fiscal intermediaries and those that may be included in the agreements. An agreement between CMS and an intermediary would specify the functions to be performed by the intermediary, which would include determining the amount of payments to be made to providers for covered services furnished to beneficiaries and making the payments, and may include other specified functions. This change was proposed because, pending the effective date of changes made by the MMA, Soc. Sec. Act §1816 does not require that the other functions set forth at 42 C.F.R. §421.100(c) through (i) be included in all intermediary agreements. The mandatory inclusion of all functions in all agreements limits CMS' ability to efficiently administer the Medicare program.

Similarly, the proposed rule would provide that some or all of the functions, which currently are mandatory for carrier contracts, may be included in carrier contracts.

Comments on the proposed rule must be received by August 16, 2005.

Proposed rule, 70 FR 35204, June 17, 2005, ¶190,001

Trends

State law requires uniform system for claim submission

by Gene' Stephens, J.D., Contributing Editor

An Amendment to House Bill 2343 under Section 4-2 of the Illinois Health Finance Reform Act, which became effective on May 2005, requires Illinois licensed hospitals and ambulatory surgical centers to adopt a uniform system for submitting patient claims and encounter data for payment from public and private payors. The Amendment requires that hospitals base their systems on the uniform electronic billing format pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), PubLNo. 104-191. Specifically, Illinois hospitals and ambulatory and surgical treatment centers must electronically submit inpatient and outpatient claims and encounter data related to surgical and invasive procedures collected for each patient no later than 60 days after the end of each calendar quarter. Ambulatory and surgical treatment centers that cannot electronically submit data may submit the requested data by computer disk until July 1, 2006.

In addition to the requirements regarding electronic patient claims and data submissions, HHS will make available on its web site a "Consumer Guide to Health Care" by January 1, 2006. The guide will include at least 30 inpatient conditions and procedures that demonstrate the highest degree of variation in patient charges and quality of care as identified by HHS. Similarly, by January 1, 2007, the guide will include 30 outpatient conditions and procedures that demonstrate the highest degree of variation in patient charges and quality of care. The Amendment also allows for the release of hospital or ambulatory and surgical treatment center identifying information absent patient identifiable information.

Senator Susan Garrett, Amendment to House Bill 2343, May 13, 2005

HHS updates Q&A on protected health information

by Gene' Stephens, J.D., Contributing Editor

The Department of Health and Human Services issued a new question and answer regarding the disclosure of protected health information (PHI). The question and answer explains the privacy rules that permit covered entities to disclose PHI to a state-designated Protection and Advocacy system without the authorization of the individual. The Protection and Advocacy system is used to protect and advocate for the rights of individuals suffering from mental illness or developmental disabilities. The question and answer further provides guidance on the standards for disclosure of PHI in cases in which a federal or state entity mandates disclosure or when the PHI is requested to carry out protection and advocacy functions.

HHS, Questions and Answers, June 20, 2005, available at http://answers.hhs.gov/