

CORRIDORS

News for North Carolina Hospitals
from the Health Care Attorneys of Poyner Spruill LLP

The Stimulus Push for Electronic Health Records and Strengthened Privacy and Security

by Pam Scott

Electronic Health Record Incentives

A significant chunk of The American Recovery and Reinvestment Act of 2009 (ARRA), approximately \$20 billion, is aimed at motivating health care providers to implement electronic health record (EHR) systems. The incentives will be paid in the form of increased Medicare and/or Medicaid payments. Medicare incentive payments will begin in 2011 and will be paid over four years for eligible hospitals and over five years for eligible health care professionals who can show "meaningful use" of a "certified EHR" system. The incentive program for hospitals is based on the "Medicare share" of a base payment amount of \$2 Million, adjusted based on the hospital's discharge data. The Medicare share takes into account the proportion of inpatient bed days that are paid by Medicare as well as an adjustment for charity care.

Hospitals and physicians who do not meet the requirements of meaningful use of certified EHRs by 2015 will be penalized through reduced Medicare payments. A significant hardship exception will be available for eligible hospitals until 2020 and for eligible professionals for up to five years.

There are three broad criteria defined in the ARRA for demonstrating that one is a meaningful EHR user: (1) meaningful use of certified EHR technology; (2) information exchange; and (3) reporting on measures using EHR. These criteria will be defined further as implementation of the new law moves forward. Meaningful users are hospitals or physician practices able to demonstrate that their EHR technology is connected in a way that improves the quality of health care through reported results in clinical quality and other measures selected



by the Secretary of Health and Human Services. Meaningful EHR use includes e-prescribing and quality reporting, and may be demonstrated by attestation, survey response, appropriate claims, quality reporting, or other manners specified by the Secretary. A key aspect of meaningful use will be the interoperability of the EHR system, i.e., how well the system talks to other systems. "Certified EHR technology" will be technology that is certified by an independent body recognized by the secretary as meeting standards for such technology, to be established by the secretary by the end of 2009.

The ARRA provides for Medicaid incentive payments, but the details of exactly how Medicare and Medicaid payments will operate together remain unclear pending the adoption of specific regulations. Hospitals may receive additional federal aid if they participate in the U.S. Department of Health and Human Services' Health Information Technology Extension Program, which is aimed at supporting and accelerating efforts to implement health care information technology in accordance with the standards, specifications and certification criteria to be established under the Health Information Technology for Economic and Clinical Health Act component of the ARRA.

On June 1, the National Committee on Vital and Health Statistics (NCVHS) issued a report of observations on meaningful use of health information technology, stemming from testimony from health care providers and

continued on page three



POYNER SPRUILL IS GOING GREEN In an effort to be more environmentally conscious, we will publish **Corridors** by email only beginning later in 2009. If you would like to continue receiving **Corridors**, please sign up by sending an email request to alerts@poyners.com with **Corridors** in the subject line.



Amendments to False Claims Act Make Failure to Return Overpayments Basis for Civil False Claim Action

by Wilson Hayman

On May 20, 2009, President Obama signed into law the Fraud Enforcement and Recovery Act of 2009 (FERA), which, among other things, amends the federal civil False Claims Act (FCA), applicable generally to conduct on or after that date. FERA is primarily aimed at reducing fraud by bringing mortgage lending businesses within the definition of “financial institutions” in the federal criminal code, and by increasing funding for enforcement agencies to pursue criminal, civil and administrative proceedings involving federal assistance programs and financial institutions by hundreds of millions of dollars. However, of primary interest to hospitals and health care providers are FERA’s amendments to the FCA, which expand liability for knowingly retaining Medicare or Medicaid overpayments and for presenting false or fraudulent claims for payment or approval.

Knowing Failure to Return Overpayments First, Section 4 of FERA provides that a hospital or other entity violates the FCA if the entity “knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the government.” The term “obligation” in this section includes “an established duty, whether or not fixed, arising... from the retention of any overpayment.” Thus, “knowingly and improperly” failing to return an overpayment, if there is an “established duty” to do so, becomes the basis for an action under the FCA. The term “improperly” is intended to limit this duty to repay by presumably excluding overpayments such as those under Medicaid that undergo a reconciliation process or those that are being appealed pursuant to Medicare appeal procedures.

The FCA has generally, in the past, been applied only to persons who knowingly filed false or fraudulent claims, i.e., persons who at the time they submitted the claims either actually knew of the claims’ falsity, acted in deliberate ignorance of their truth or falsity, or acted in reckless disregard of their truth or falsity. Such is clearly no longer the case. Because of the interpretation and application of existing statutes, regulations and provider contracts regarding retention of overpayments, this involves an “established duty” or “obligation” that may now trigger the FCA. Although this provision is not expressly made retroactive, the government will likely argue that it should apply to overpayments made before the date of the legislation. These amendments also give the federal

authorities a weapon in their arsenal to enforce the federal physician self-referral or Stark law in addition to civil monetary penalties.

Expanded Liability for Claims Affecting Government Funds

Second, FERA attempts to close certain loopholes created by recent court decisions that Congress viewed as undermining or limiting the scope of the FCA. Prior to FERA, the FCA provided that a person is liable if he “knowingly makes, uses, or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the Government.” Recent decisions had interpreted the FCA as requiring the federal government to prove that a defendant intended the government itself to pay a claim, so that a subcontractor would have no liability unless it submitted its claims to the government, not to a general contractor, for payment, even if the claims had been paid by government funds. A Senate Report noted that defendants have argued that these decisions precluded liability under the FCA for Medicaid claims submitted to a state government. Accordingly, FERA deleted any requirement for liability that an entity directly present a claim to the government, so that an entity may now incur liability if it “knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval.” In addition, an entity now may also be liable if it “knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim.” This latter amendment applies to all claims under the FCA pending on or after June 7, 2008.

FERA now creates liability under the FCA for the knowing failure to return overpayments, and it makes the FCA clearly applicable to government funds distributed by states or intermediaries rather than directly from the federal government. The amendments also require violators to reimburse the federal government for the costs of a civil action to recover penalties or damages. With these increased liabilities and strengthened tools for enforcement, hospitals and providers are urged to review their self-audit and compliance policies and programs in these areas.

For more information on hospital compliance or other health care law issues, please contact Wilson Hayman at 919.783.1140 or whayman@poynerspruill.com.

The Stimulus Push... continued from page one

other stakeholders at recent public hearings on the issue of meaningful use. In its report, NCVHS stressed several common themes that were addressed by most of the stakeholders who testified. These included a focus on how EHR technology can be used effectively to achieve quality outcomes, health status improvement and cost controls rather than on the mere acquisition of EHR technology; the need for clear and predictable milestones for phased transition toward the ultimate goals of effective EHR technology and meaningful use of EHR; the need for EHRs to effectively support patient-centered care, care coordination and population/public health management; additional work needed to harmonize key standards for EHR; and the importance of addressing public trust issues by making privacy and security policies an integral part of meaningful use of EHR technology. In its observational report, NCVHS noted that there appeared to be an information gap with regard to how hospitals would achieve meaningful use of EHR technology. The report indicated that the stakeholder discussion focused on the use of EHRs by physicians and other eligible professionals, but that more information is needed to fully understand hospital EHR capacity and the functionality of EHRs in the hospital setting.

Some providers have questioned whether the incentives and penalties established by the ARRA will be enough to encourage everyone to jump on the EHR bandwagon, given the significant time, expense and effort involved in developing and implementing EHR systems. Certainly, providers who are already in the process of developing/adopting an EHR system will likely slow those projects somewhat until certification requirements and “meaningful use” are more clearly defined. The Health IT Policy and Health IT Standards Committees are expected to release recommendations on the definition of “meaningful use” within about a month and complete an initial set of standards by the end of this year.

HITECH

In addition to the ARRA provisions encouraging health care providers to adopt EHR systems, a separate component known as the Health Information Technology for Economic and Clinical Health Act (HITECH), is aimed at strengthening the privacy and security of all health records. HITECH’s requirements will significantly alter privacy and security compliance obligations of covered entities and business associates. There remains a good deal of uncertainty regarding the details of the privacy and security changes to come under HITECH, due to regulations that have yet to be developed. However, there are a number of significant changes included in HITECH that are clearly defined in the law and will alter the landscape of health care information privacy and security.

HITECH establishes new breach notification requirements applicable to covered entities and their business associates when breaches of unsecured PHI occur. Covered entities are required to notify individuals in writing if their PHI is disclosed, lost or otherwise compromised. In addition, following the discovery of a breach by a business associate, the business associate must notify the covered entity of the breach and identify the individuals whose unsecured PHI has been or is reasonably believed to have been breached. HITECH requires notifications to be made without unreasonable delay, within 60 calendar days after discovery of the breach. If the breach involves 500 or more individuals, the covered entity must also inform HHS and prominent media outlets serving the area in question. There are exceptions for cases in which: (1) the breach is unintentional and made by an employee or individual acting under authority of a covered entity or business associate if the PHI was acquired, accessed or used in good faith and within the scope of employment or other professional relationship, and was not further accessed, used or disclosed; or (2) an inadvertent disclosure occurs by an individual authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility, provided the PHI is not further accessed, used or disclosed without authorization.

On April 17, 2009, HHS issued a guidance specifying the technologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals. The guidance was developed through a joint effort by the HHS Office for Civil Rights, the Office of the National Coordinator for Health Information Technology, and the Centers for Medicare and Medicaid Services. It relates to two breach notification regulations to be adopted pursuant to HITECH: one to be issued by HHS for covered entities and business associates under HIPAA (discussed above); another to be issued by the Federal Trade Commission for vendors of personal health records and other non-HIPAA-covered entities. If the entities subject to regulation apply the technologies and methodologies specified in the guidance to secure information, they will not have to make the notifications required by the regulations in the event the information is breached. In other words, use of the methodologies and technologies specified in the guidance to secure PHI through encryption or destruction essentially creates a safe harbor for covered entities and their business associates, eliminating the need to provide the required breach notifications that apply only to breaches of unsecured PHI. The guidance will apply to breaches 30 days after publication of the interim final rules. The requirements for methodologies and technologies to render PHI unusable, unreadable or indecipherable eventually will be adopted as a formal rule following HHS’s consideration of comments regarding the initial guidance.

Another major change under HITECH is that business associates will be directly subject to HIPAA Privacy and Security Rules, which means that starting February 17,

continued on page five



EMTALA Update: CMS Issues Guidance Clarifying Recent Changes

by Jessica Lewis

In March of this year, the Centers for Medicare and Medicaid Services (CMS) issued guidance clarifying three changes to the Emergency Medical Treatment and Labor Act (EMTALA) included in the 2009 Inpatient Prospective Payment System (IPPS) Final Rule. These significant changes involve community call plans, EMTALA waivers in times of national emergency and transfer obligations related to hospitals with specialized capabilities, as discussed in more detail below.

Community Call Plans Pursuant to 42 CFR § 489.24(j)(2)(iii), a hospital may participate in formal community call plans with other hospitals to share on call responsibilities. If a hospital chooses to participate in a community call plan, the plan must:

- clearly define when each hospital is responsible for on call coverage and what services it will cover;
- describe the geographic area encompassed by the plan;
- contain documentation that local and regional EMS systems include information on the arrangements under the plan;
- contain a statement that an individual seeking emergency treatment at a hospital not designated as the on-call hospital will nevertheless receive a medical screening exam and stabilizing treatment within the capability of the hospital;
- contain a statement that participating hospitals will appropriately transfer patients in accordance with the EMTALA regulations;
- be assessed annually; and
- be signed by a representative of each hospital participating in the plan.

CMS also points out that hospitals which participate in community call plans must still have backup plans for times when the community call plan is nonoperational.

CMS is quick to note that participation in a community call plan does not relieve a hospital of its obligations to any individual who comes to its dedicated emergency department. Regardless of whether the hospital is the one designated at that time for the service sought, it must provide screening and stabilization within its capability and/or arrange for an appropriate transfer. A transfer would generally be appropriate if an individual presented to one hospital with an emergency medical condition that required the attention of a specialist on call at another hospital.

Hospitals are also required by EMTALA to maintain lists of on call physicians. If a hospital chooses to participate in a community call plan, its on call list should include not only physicians who are members of that hospital's medical staff, but also physicians at other participating hospitals who are on call under the community plan to provide specialty services to stabilize patients.

Emergency Waiver During a national emergency, the Secretary of the Department of Health and Human Services (HHS) may temporarily waive EMTALA sanctions for the inappropriate transfer of an unstabilized patient or the diversion of a patient with an emergency medical condition to another location for a medical screening exam, in order to allow hospitals to implement their disaster plans to provide health care services in a disaster area. When a hospital activates its disaster plan and uses emergency waivers from HHS, it must notify the appropriate state agency (the North Carolina Department of Health and Human Services) so that CMS can track the number and locations of hospitals using waivers.

Specialized Capabilities Last year, CMS issued a proposed rule that would require a hospital with specialized capabilities to accept the transfer of an unstable patient, even though the patient had been admitted to the first hospital where he or she presented with an emergency medical condition, as long as the receiving hospital had the capacity to treat the patient and the transfer was appropriate. This proposed rule was not adopted. Instead, CMS has now clarified that EMTALA obligations end once a patient with an emergency medical condition, even if unstable, is admitted in good faith to a hospital as an inpatient. A hospital with specialized capabilities that might receive the same patient as a transfer is not subject to EMTALA obligations regarding that transfer. A word of caution is appropriate, however – if a patient with an unstable emergency medical condition is not actually admitted to the first hospital, and transfer to a second hospital with specialized capabilities is sought, then EMTALA obligations do apply to the second hospital involved in the transfer.

For more information on CMS limits or other health care law related issues, please contact Jessica Lewis at 919.783.2941 or jlewis@poynerspruill.com.

The Stimulus Push...

continued from page three

2010 they must implement the administrative, physical and technical safeguards of the Security Rule, and they may use and disclose PHI only as allowed by the Privacy Rule. Business associates will be subject to penalties for violating the HIPAA Privacy and Security Rules. Currently, business associates are contractually bound to comply with applicable HIPAA privacy and security measures pursuant to business associate agreements with the covered entities with which they work. However, under HITECH, business associates will be statutorily required to comply with the HIPAA Privacy and Security Rules and will be subject to penalties for failing to do so.

Additional changes under HITECH include the following:

- Individuals with sensitive health conditions they want to keep confidential, even from their insurance carriers, can request that disclosure of information regarding their health be kept confidential, provided the patient is willing to pay for care out of pocket. Covered entities must comply with requested restrictions of treatment, payment and operations (TPO) disclosures to health plans and not report the information at issue if it is not related to treatment and the patient paid in full, out of pocket.
 - A covered entity using or disclosing PHI, or requesting PHI from another covered entity, must limit “to the extent practicable” disclosure to the limited data set as defined under HIPAA, or, if more information is needed, to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. A limited data set is PHI from which facial identifiers have been removed, such as names, addresses, Social Security numbers, etc. The forthcoming guidance from HHS (expected by August 2010) on the details of this new disclosure threshold will determine the significance of this new requirement.
 - Covered entities must be able to account for TPO disclosures of PHI used or maintained in an EHR system for three years prior to the date of a request, in electronic form.
 - A patient will receive requested PHI in electronic format if the covered entity uses or maintains an EHR. The patient may designate another person to receive the transmittal without an authorization. The covered entity may only charge a fee commensurate with its labor costs providing the PHI.
- Covered entities and business associates are expressly prohibited from selling electronic PHI without valid authorization, except under certain conditions.
 - More stringent enforcement measures, including tiered penalties for HIPAA violations based upon an offender’s level of knowledge and actions taken to correct the violation; mandatory penalties for HIPAA violations due to “willful neglect”; and required formal HHS investigation of any complaints initially determined to involve willful neglect.
 - State attorneys general may bring state actions to enforce HIPAA, seeking statutory damages and attorneys’ fees for violations. Previously, such enforcement was limited to the Office of Civil Rights within HHS.

The privacy and security changes required under HITECH provide a good opportunity for hospitals and other health care providers to dust off their HIPAA policies and procedures and re-examine them to ensure they effectively address today’s privacy and security concerns and challenges. Providers who already have a comprehensive HIPAA compliance plan will have a good foundation on which to build for purposes of meeting the new HITECH requirements. Even though business associates will now be required by statute to comply with the HIPAA Privacy and Security Rules, business associate agreements are still required, so hospitals and other covered entities will need to modify their existing business associate agreements to address the new compliance obligations highlighted above.

As discussed above, a number of significant health care information changes are on the horizon in the areas of electronic health records and stepped-up privacy and security, but compliance planning will depend in large part upon details that have yet to be determined. Stay tuned to *Corridors* for future updates on meaningful use of certified EHRs and new health information privacy and security requirements under HITECH.

For more information on HIPAA or other health care law related issues, please contact Pam Scott at 919.783.2954 or pscott@poynerspruill.com.

We’re Award Winners!

Poyner Spruill was given a “Your Honor Award” by the Legal Marketing Association (LMA) at the recent 2009 Annual Conference held in National Harbor, Md. We took top honors in the promotional and collateral material category for our suite of health care industry newsletters. *Corridors: News for North Carolina Hospitals*, *Shorts on Long Term Care*, and *Hospice EndNotes* won as a package of collateral material for providing readership value and promoting the firm’s robust health care practice. Editors Wilson Hayman, Ken Burgess, and Mike Hale oversee each issue of their respective publications with an eye toward providing fresh content and thought leadership for each of these niche health care markets. Congratulations to *Corridors* editor Wilson Hayman!



“Red Flag Rules” Will Impose Additional Administrative Burdens on Hospitals

By Kevin Ceglowski

In 2007, the Federal Trade Commission (FTC) issued “Red Flag Rules,” which require financial institutions and other creditors that maintain covered accounts to develop and implement identity theft prevention programs. These Red Flag Rules likely apply to hospitals and other health care providers. The original deadline for creditors to comply with the Red Flag Rules was November 1, 2008, but this deadline has been extended several times. Creditors must now comply by August 1, 2009.

According to the FTC’s definition, a creditor is any entity that regularly extends, renews or continues credit; any entity that regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew or continue credit. A covered account is an account used mostly for personal, family or household purposes and that involves multiple payments or transactions. A covered account is also any account for which there is a foreseeable risk of identity theft. Although some issues surrounding the definition of creditor are not yet resolved, the FTC has taken the position that a hospital or other health care provider that bills for services after they are rendered or that accepts insurance but holds the customer ultimately responsible for payment is a creditor subject to the Red Flag Rules.

A “Red Flag” is a pattern, practice or specific activity that indicates the possible existence of identity theft. Examples of Red Flags include:

- documents provided for identification appear to have been altered or forged;
- information on the identification provided by a person is not consistent with information provided by that person when making a credit application;

- an application appears to have been altered or forged or gives the appearance of having been destroyed and reassembled; and
- a person opening a credit account fails to provide all required personal identifying information.

The Red Flag Rules require a covered entity to develop and implement a written identity theft prevention program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Red Flag Rules are flexible, and they allow the creditor to develop a program that is appropriate to the size and complexity of the company and the nature and scope of its activities. The program must include reasonable policies and procedures to:

- identify Red Flags;
- detect Red Flags;
- respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- ensure that the program is updated periodically to reflect changes in risks to customers and the business from identity theft.

Hospitals should begin preparing to comply with the Red Flag Rules by developing an identity theft prevention program in advance of the August 1, 2009, deadline. Given the stringent HIPAA privacy requirements that hospitals and other health care providers must comply with, there may already be systems in place that satisfy some of the Red Flag Rules. In developing the required program, hospitals should consider Red Flags most likely to present themselves in the health care industry, such as claims that services billed for were not actually provided, claims that services were billed under the wrong patient name, inconsistencies between records of treatment and a physical examination of a patient, and claims that a patient or the party billed has been a victim of identity theft. Hospitals should also incorporate procedures into their programs for carefully verifying insurance coverage information and change of address requests.

Although the details of each hospital’s program will vary based on the particular nature of its business, these guidelines should provide a starting point for developing the required identity theft prevention program. Hospital administrators should monitor the status of the Red Flag Rules in advance of the August 1, 2009 effective date and ensure that they have a program in place by the deadline if there are no further delays in the application of the rules.

For more information about employment law related issues, please contact Kevin Ceglowski at 919.783.2853 or kceglowski@poynerspruill.com.