
HEALTH CARE PRACTICE GROUP CLIENT NEWSLETTER

In This Issue:

Massachusetts Enacts New Regulations for the Protection of Residents' Personal Information.	1
OCR Provides Guidance on Communications under the HIPAA Privacy Rule.	5
Massachusetts Court of Appeals Grants Physician New Trial in Medicaid Fraud Case.	7
OIG Advises Against Joint Venture Arrangement Between Physician Practice Groups and Free-Standing Facility	8
Joint Commission Issues Sentinel Event Alert on Anticoagulants.	10
OIG Releases Fiscal Year 2009 Work Plan.	11

The Rogers Law Firm

100 Cambridge Street
20th Floor, Suite 2000
Boston, MA 02114
617.723.1100

www.therogerslawfirm.com

Wilson D. Rogers, Jr.
Peter Pommersheim
Michael J. Fazio, Jr.
Wilson D. Rogers, III
Francis J. O'Connor
Mark C. Rogers
Megan M. Grew
Robert E. Driscoll, Jr.

Massachusetts Enacts New Regulations for the Protection of Residents' Personal Information

In September of 2007, Massachusetts enacted "An Act Relative to Security Freezes and Notification of Data Breaches" (the "Act")¹, requiring companies, entities or people possessing personal information to take affirmative steps in the wake of a security breach. The Act became effective on February 3, 2008, increasing healthcare organizations' exposure to civil actions by individuals and the Massachusetts Attorney General ("AG") with regard to the security of their patient and employment records. Specifically, the Act requires the company or entity to provide notice to affected Massachusetts residents whose personal information has been subject to a security breach. The Act also includes requirements for requesting security freezes and data destruction, and directs a state agency to adopt regulations directed at safeguarding personal information. Pursuant to the Act, the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") released new regulations² on September 22, 2008, ordering any companies, entities, or people with Massachusetts residents' personal information to implement requirements protecting that information.

The scope of the regulations is broad, applying to all persons, companies or entities that own, license, store or maintain personal information about residents of the Commonwealth of Massachusetts, regardless of whether or not the entity has operations in the Commonwealth. "Personal information" is limited to a resident's first and last

¹ M.G.L. c. 93H.

² 201 CMR 17.00 *et seq.*

name or first initial and last name in combination with a Social Security number, driver's license number or financial account number. The regulations impose two principal requirements: (i) the duty to develop, implement and maintain a very comprehensive written information security program that meets very specific requirements; and (ii) the obligation to meet specific computer information security requirements.

The regulations require all companies that handle personal information to encrypt data stored on laptops, monitor employee access to data and take other steps to protect customer information. For example, the regulations dictate conduct in vendor and employee relationships, including limiting employees with access to sensitive information to those who need access to do their jobs. The regulations also force an entity to identify every record (whether paper or electronic) that has personal information, and compel specific electronic security measures, including for wireless networks. They also require entities to obtain written certifications from service providers that will be provided with personal information before those vendors start their work. For most organizations, the regulations will require major operational and administrative changes. The new regulations become effective January 1, 2009.

People, companies and entities subject to the regulations must develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing personal information. The information security program must be reasonably consistent with industry standards, and it must also contain administrative, technical and physical safeguards to ensure the security and confidentiality of such records.

The regulations specify the following factors to be taken into account when determining whether a program is in compliance: (i) the size, scope and type of business of the entity or person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such entity or person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information. While the measure calls for consistency with applicable federal regulations, the regulations include some items that overlap with the Federal Trade Commission ("FTC") Safeguards Rule, the HIPAA Security Rule and other federal agency guidance, but they also go far beyond what is currently required under federal law. Entities covered by the new regulations must have an information security program that requires the entity to:

- **Designate Responsible Employees.** Designate one or more employees to maintain the comprehensive information security program.
- **Identify Risks and Assess Safeguards.** Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing personal information, and evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.
- **Develop Employee Security Policies.** Develop security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.
- **Impose Disciplinary Measures.** Impose disciplinary measures for violations of the comprehensive information security program rules.

- **Prevent Access to Personal Information by Former Employees.** Prevent terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.
- **Exercise Control over Service Providers.** Take reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain such safeguards. *Prior to* permitting third-party service providers access to personal information, the person permitting such access shall obtain from the third-party service provider a *written* certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations.
- **Place Appropriate Limits on the Collection and Use of Personal Information.** Limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limit the time such information is retained to that reasonably necessary to accomplish such purpose; and limit access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.
- **Identify Records with Personal Information.** Identify paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information.
- **Restrict Physical Access.** Implement reasonable restrictions on physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; store such records and data in locked facilities, storage areas or containers.
- **Conduct Regular Monitoring.** Conduct regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrade information safeguards as necessary to limit risks.
- **Conduct Annual Reviews.** Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- **Document Responsive Actions for Breaches.** When a breach incident occurs, document responsive actions taken, conduct a mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

In addition to the requirements to implement a detailed information security program, the new regulations also mandate specific computer system security requirements. Encryption is defined in the regulations as a method “at least as secure” as one that transforms data “into a form in which meaning cannot be assigned without the use of a confidential process or key.” Each

covered party must establish and maintain a security system, covering all of its computers (including any wireless system), which, at a minimum, has the following elements:

- **Secure user authentication protocols including:** control of user IDs and other identifiers; a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; restricting access to active users and active user accounts only; and blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- **Secure access control measure:** restricting access to records and files containing personal information to those who need such information to perform their job duties; and assigning unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
- **Encryption requirement in transmission:** to the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly;
- **Reasonable monitoring of systems:** monitoring for unauthorized use of or access to personal information;
- **Encryption requirement in stored information:** encryption of all personal information stored on laptops or other portable devices;
- **Firewall protection:** for files containing personal information on a system that is connected to the Internet, the system must have reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information;
- **Malware and virus protection:** the system must have reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and
- **Education and training:** each covered entity must train employees on the proper use of the computer security system and the importance of personal information security.

It is important to note that the Massachusetts regulations require the safeguards contained in the information security program be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations to which the person or entity that owns, licenses, stores or maintains such information is subject.

In addition to compliance with the Massachusetts regulations from OCABR, organizations should be aware that the FTC recently issued a reminder of the upcoming November 1, 2008, compliance deadline for implementing identity theft prevention programs pursuant to the identity theft red flag rules (“Red Flag Rules”). Under the Red Flag Rules, creditors that are subject to FTC enforcement under the Fair Credit Reporting Act (“FCRA”) with “covered accounts” must implement programs that identify, detect and respond to practices that could indicate identity theft. It is likely that health care providers are subject to the Red Flag Rules because they (1) are

creditors³, (2) are subject to enforcement by the FTC under the FCRA⁴, and (3) have “covered accounts.”⁵ The Red Flag Rules mandate that a covered entity’s program should detect, prevent and mitigate identity theft in connection with covered accounts and should “include reasonable policies and procedures to” accomplish the following: 1) identify accounts which may be susceptible to instances of medical identity theft; 2) detect red flags by authenticating patients and monitoring transactions; 3) make appropriate responses that prevent and mitigate identity theft; 4) ensure the program is updated to reflect changing risks to patients for identity theft; and 5) ensure approval by the entity’s board of directors for the identity theft prevention program and maintain oversight, development implementation and administration of the program.

Similar to HIPAA, the Red Flag Rules give covered health care providers some flexibility in implementing their identity theft programs, taking into account the size and complexity of a health care provider's business. Thus, the program developed in compliance with the Red Flag Rules may be part of a provider’s HIPAA compliance efforts. In fact, there is significant overlap between the requirements of HIPAA and the Red Flag Rules, and many of the above actions already may have been included in an organization’s HIPAA compliance efforts. Nevertheless, providers should undertake a review of their identity theft prevention programs to ensure compliance with both HIPAA and the Red Flag Rules, as well as the Massachusetts data protection regulations.

Due to the detailed requirements of the new Massachusetts data protection regulations and the approaching compliance deadline, all entities that own, license, store or maintain Massachusetts residents’ personal information should commence a review of their current security policies and procedures to determine whether they are and will be in compliance as of the January 1, 2009, effective date. If you have any questions regarding the new regulations, please do not hesitate to contact any of the attorneys at The Rogers Law Firm.

OCR Provides Guidance on Communications under the HIPAA Privacy Rule

The Office for Civil Rights (“OCR”) of the United States Department of Health and Human Services (“HHS”) recently issued a guide explaining when a health care provider is allowed to share a patient’s health information with the patient’s family members, friends, or others identified by the patient as involved in the patient’s care under the HIPAA Privacy Rule. The guide, which is entitled “Communicating With a Patient’s Family, Friends or Others Involved in

³ A “creditor” includes any person or entity that “regularly extends, renews, or continues credit.” The term “credit” means “the right granted by a creditor to a debtor to defer payment of debt or ... to purchase ... services and defer payment therefor.”

⁴ Creditors subject to FCRA enforcement include any person, including a corporation, that violates the FCRA “irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests” of the FTC Act. Thus, although the FTC Act allows the FTC to govern only corporations that operate “for profit” (as well as nonprofit trade associations and professional societies that provide economic benefits to their for-profit members), the FCRA contains no such similar restriction. Accordingly, a nonprofit corporation likely would be subject to FTC enforcement under the FCRA and, likewise, may be subject to the Red Flag Rules.

⁵ A “covered account” is defined as (a) an “account ... primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions”; or (b) “[a]ny other account ... for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the ... creditor from identity theft.”

the Patient's Care" (the "Guide"), is in the form of questions and answers. The following is an overview of the important information included within the Guide.

- If a patient is present and has the capacity to make health care decisions, a health care provider may discuss the patient's health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object. A health care provider may also share information with these persons if, using professional judgment, he or she decides that the patient does not object. As an example, the Guide states that an Emergency Room doctor may discuss the patient's treatment in front of the patient's friend if the patient asks the friend to come into the treatment room.
- If a patient is not present or is incapacitated, a health care provider may share the patient's information with the patient's family, friends, or others as long as the health care provider determines, based on professional judgment, that it is in the best interest of the patient. However, when someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asks the person to be involved in his or her care or payment for care. As an example, the OCR states that a surgeon who performed emergency surgery on a patient may tell the patient's spouse about the patient's condition while the patient is unconscious.
- HIPAA does not require that a health care provider document the patient's decision to allow the provider to share his or her health information with a family member, friend, or other person involved in the patient's care or payment for care.
- When a health care provider is allowed to share a patient's health information with a person, such information may be shared face to face, over the phone, or in writing.
- If a patient's family member, friend, or other person involved in the patient's care or payment for care calls the health care provider to ask about the patient's condition, HIPAA does not require the health care provider to obtain proof of who the person is before speaking with them.
- HIPAA allows health care providers to use professional judgment and experience to decide if it is in the patient's best interest to allow another person to pick up a prescription, medical supplies, x-rays, or other similar forms of information for the patient.
- A health care provider is permitted under HIPAA to share a patient's health information with an interpreter in order to communicate with the patient or with the patient's family, friends, or others involved in the patient's care or payment for care. The interpreter, however, needs to be an individual who is either employed by the provider, has a written contract or other agreement with the provider to provide interpretive services, or is the patient's family member, friend, or other person identified by the patient as his or her interpreter.

It is important to remember that the HIPAA Privacy Rule is preempted by Massachusetts law to the extent that a particular Massachusetts statute or regulation pertaining to health information privacy is more stringent than the corresponding HIPAA Privacy Regulation.

If you have any questions regarding the Guide, or whether a particular HIPAA Privacy Regulation is preempted by Massachusetts law, please do not hesitate to contact any of the attorneys at The Rogers Law Firm.

Massachusetts Court of Appeals Grants Physician New Trial in Medicaid Fraud Case

On September 17, 2008, the Massachusetts Court of Appeals granted Dr. Kennard Kobrin a new trial following his conviction for Medicaid fraud. The court based its determination on evidence that the charges were submitted and paid by Medicare and the state Medicaid program was never billed for the services at issue. Although this holding may relieve Dr. Kobrin of penalties under state statutes protecting against Medicaid fraud, he is susceptible to federal charges based on Medicare regulations.

In 1998, a grand jury returned sixteen (16) indictments against Dr. Kobrin on eighty-two (82) counts relating to Medicaid fraud¹ and illegally prescribing controlled substances². Kobrin was then acquitted of all but three (3) counts including: one (1) count of illegally prescribing a Class C controlled substance to a patient of long standing; and two (2) counts of Medicaid fraud for ordering unnecessary psychological testing.

After his appeal, the Massachusetts Court of Appeals reversed the conviction for illegally prescribing a controlled substance. The court held that the evidence was insufficient to sustain criminal liability under the Massachusetts Controlled Substances Act (the “Act”). The Act requires proof beyond a reasonable doubt that the physician did not have a legitimate medical objective in prescribing the drug. The court further held that a mere demonstration of failure to comply with accepted medical practice is a basis for negligence or medical malpractice rather than criminal liability.

The Medicaid fraud claims related to Dr. Kobrin’s involvement in an arrangement by which he leased office space to psychologists at a high rental rate and in exchange referred patients to them for medically unnecessary testing. The appeals court held that the trial court properly ordered a new trial on the basis that no bills were actually submitted to Medicaid for the suspect testing services. The patients who received the unnecessary testing were beneficiaries of both Medicare and Medicaid and it was Medicare that was billed for the services. Despite the state’s contention on the issue of fraud and the submission of signed referrals with false statements, the court maintained that the statutory purpose of the Medicaid fraud regulations is to “deter and punish fraud that brings about the unwarranted disbursement of limited Medicaid resources.”³ Therefore, based on the lack of evidence that the claims were actually submitted to Medicaid, the court found that there was no basis for a conviction of Medicaid fraud under state law.

¹ M.G.L. c. 188E, §§ 40, 41.

² M.G.L. c. 94C, § 32B(a).

³ *Massachusetts v. Kobrin*, 72 Mass. App. Ct. 589, 2008.

OIG Advises Against Joint Venture Arrangement Between Physician Practice Groups and Free-Standing Facility

On August 26, 2008, the Office of Inspector General (“OIG”) of the United States Department of Health and Human Services issued a new Advisory Opinion (Advisory Opinion 08-10), advising that a joint venture lease arrangement between physician practice groups and a free-standing facility could potentially generate prohibited remuneration under the Anti-Kickback Statute. This article provides an overview of the Advisory Opinion.

Background

Advisory Opinion 08-10 applies to a proposed arrangement between a physician group practice that provides cancer treatment services in a free-standing facility (“Facility”) and other physician groups specializing in urology in the same geographical area (“Urologist Groups”) which participate in the Medicare program. The Facility provides a range of cancer treatments including intensity-modulated radiation therapy (“IMRT”) which is commonly used to treat prostate cancer patients referred to the Facility by urologists. The Urologist Groups do not provide IMRT and do not own facilities with the capability to provide such treatment. The Urologist Groups refer most of their prostate cancer patients to the Facility and the remainder to a competing facility.

The Facility proposes to lease the space, equipment, and personnel services necessary to perform IMRT to the Urologist Groups by a series of written agreements. The Facility would provide the Urologist Groups with supplies and billing services and its radiologists who normally perform services billed by the Facility would enter contracts with the Urologist Groups to supervise the IMRT procedures as independent contractors. In exchange for these provisions, the Urologist Groups would pay rental fees at fixed amounts, set in advance in accordance with fair market value.

The technical and professional components of IMRT services provided to Medicare beneficiaries at the Facility are currently billed under the Facility billing number. Under the proposed agreement, these components would be billed to Medicare using the billing numbers of the Urologist Groups. The Urologist Groups would pay the lease amounts regardless of the number of patients referred to the Facility but would retain the difference between the fees collected from Medicare and the amounts owed under the lease agreements.

OIG Analysis

In examining this arrangement, the OIG found that the agreement would essentially establish a joint venture between the Facility and the Urologist Groups. The OIG points to the potential concerns for joint ventures between a group in a position to refer business and those who furnish items or services paid by Medicare or Medicaid. These concerns were set forth in its Special Advisory Bulletin on Contractual Joint Ventures¹ which describes a similar arrangement as a suspect joint venture. The Special Advisory Bulletin example arrangement describes an agreement in which the owner contracts out almost the entire operation of a related line of business to the supplier, otherwise a potential competitor, and receives in return the profits of the business as remuneration for its federal program referrals.

¹ 68 FR 23148 (2003).

The OIG highlights that the Facility would be expanding into a business which is dependent on referrals from the Urologist Groups and would have little financial, capital or human resources to commit and therefore would assume little risk. The OIG finds this suspect because this would position the Urologist Groups to ensure the success of the business, not only by referrals to the Facility for IMRT but also by choosing IMRT over other available treatments. The OIG then enumerates other characteristics of the proposed arrangement described in the Special Advisory Bulletin which include the following:

- The Facility is an established provider of the very services that the Urologist Groups would provide through the arrangement and is in the position to directly provide the IMRT in its own right, billing Medicare in its own name, and retaining all available reimbursement.
- The Urologist Groups would use the premises, equipment and staff of the Facility to serve its own patient base- the very patients some of the groups have historically referred to the Facility or other outside suppliers for the same services.
- The aggregate income to the Urologist Groups would vary with referrals to the Facility, and, because the various agreements could be tailored to fit the historical pattern of referrals by the Urologist Groups, so might the income to the Facility.
- The Facility (and its radiologists engaged as independent contractors) and the Urologist Groups would share in the economic benefit of the IMRT.

Based on these elements, the OIG concludes that this may allow the Facility to pay the Urologist Groups a share of the profits from their IMRT referrals. This would mean the Facility is agreeing to provide services it could otherwise provide in its own right for less than the available reimbursement and is potentially providing a referral source, the Urologist Groups, with the opportunity to generate a fee and a profit.

Such an arrangement would violate the Anti-Kickback Statute by rewarding the Urologist Groups for their referrals. The Anti-Kickback Statute makes it a criminal offense to knowingly and willingly offer, pay, solicit or receive any remuneration to induce or reward referrals of items or services reimbursable by a Federal health care program.² The OIG finds that this agreement does not fall within any of the safe harbor exceptions to the Anti-Kickback Statute and states that even if the component agreements could satisfy the conditions of the space and equipment rental safe harbors or the personal services and management contracts safe harbor, those exceptions would only protect remuneration paid by the Urologist Groups to the Facility rather than the potential compensation to the Urologist Groups making the referrals. By allowing the Urologist Groups the opportunity to generate a fee for the services that the Facility could otherwise provide, the OIG considers this remuneration that would implicate the Anti-Kickback Statute.

Conclusion

The OIG clarifies that a final conclusion of this agreement as violative of the Anti-Kickback Statute would require a determination of the parties' intent which is beyond the scope of the Advisory Opinion. However, the legal analysis points to a suspect arrangement in which the Facility contracts services to allow remuneration to the Urology Groups for the referrals they provide.

² Social Security Act § 1128B(b).

Joint Commission Issues Sentinel Event Alert on Anticoagulants

On September 24, 2008, the Joint Commission issued a Sentinel Event Alert¹ (the “alert”) aimed at preventing medication errors associated with commonly used blood thinners known as anticoagulants. The alert comes in response to a number of recent high profile errors related to commonly used anticoagulants which highlights a safety issue that too frequently results in harm or even death to patients.

The Joint Commission’s new alert urges greater attention to the dangers associated with anticoagulants, life-saving medications that also present serious risks when administered incorrectly or in error. The Joint Commission stated that patients being treated with these medications must be closely monitored and screened for drug and food interactions, given that commonly used anticoagulants such as heparin and warfarin have narrow therapeutic ranges and a high potential for complications.

The alert highlights factors that contribute to anticoagulant medication errors, including lack of standardized labeling and packaging, failure to document and communicate patient instructions during hand-offs, and inappropriate dosing for pediatric patients. To reduce the risk of errors related to commonly used anticoagulants, the alert recommends that health care providers take a series of specific steps, including the following:

- Assess the risks of using anticoagulants.
- Use best practices or evidence-based guidelines regarding anticoagulants.
- Establish standard dose limits on anticoagulants and require that a doctor confirm any exceptions.
- Clearly label syringes and other containers used for anticoagulants.
- Clarify all anticoagulant dosing for pediatric patients, who are higher risk because these drugs are formulated and packaged for adults.

Other strategies for reducing the errors related to anticoagulants include staff communication and collaboration; patient education and participation; designating pharmacists to manage anticoagulant services; and use of computerized physician order entry and bar coding technology, if available.

If you should have any questions regarding The Joint Commission’s Sentinel Event Alert, please do not hesitate to contact any of the attorneys at The Rogers Law Firm.

¹ The Joint Commission: Preventing errors relating to commonly used anticoagulants. *Sentinel Event Alert #41*, September 24, 2008. Available online: http://www.jointcommission.org/SentinelEvents/SentinelEventAlert/sea_41.htm (last accessed 10/10/08).

OIG Releases Fiscal Year 2009 Work Plan

On October 1, 2008, the Office of Inspector General (“OIG”) of the United States Department of Health and Human Services (“HHS”) released its Fiscal Year 2009 Work Plan (the “Work Plan”). The Work Plan sets forth the OIG priorities for the upcoming fiscal year in preventing and detecting fraud and abuse for the programs and operations of HHS. The Work Plan identifies Durable Medical Equipment (“DME”) as the top priority for the upcoming fiscal year. Specifically, the OIG will be examining Medicare Part B claims for DME, prosthetics, orthotics and supplies that are furnished to beneficiaries receiving home health services.

In addition to DME, the Work Plan identifies several other areas of focus for the OIG, particularly with respect to hospitals. The following is an overview of several of the OIG’s planned investigative projects for hospitals in the upcoming fiscal year:

- Appropriateness of Medicare Inpatient Capital Payments (such payments reimburse a hospital’s expenditures for assets, such as equipment and facilities);
- Whether Medicare Capital Payments (payments made to hospitals if they incur unanticipated capital expenditures in excess of \$5 million due to extraordinary circumstances beyond their control, such as a flood, fire or earthquake) were made in accordance with Federal requirements;
- Whether hospitals improperly claimed provider-based status for inpatient and outpatient facilities;
- Appropriateness of Medicare reimbursement to hospital-owned physician practices that have provider-based designation; and
- Whether hospitals have complied with Medicare requirements for reporting wage data used to calculate wage indices for the Inpatient Prospective Payment System.

In addition to the above investigations, the OIG also plans to review the incidences of and payments for serious medical errors or “never events”.

If you have any questions with respect to the Work Plan, please do not hesitate to contact any of the attorneys at The Rogers Law Firm.

IRS CIRCULAR 230 DISCLOSURE: To ensure compliance with requirements imposed by the Internal Revenue Service, we inform you that any U.S. federal tax advice contained within this communication (including any attachments) was not intended or written to be used, and cannot be used, by any person for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

This Newsletter is published by The Rogers Law Firm to keep its clients informed of developments in health law. The Newsletter should not be construed or relied upon as legal advice or legal opinion on any specific facts or circumstances. If you have any questions or concerns regarding the articles contained in the Newsletter or would like legal advice or legal opinion concerning a specific matter, please do not hesitate to contact any of the attorneys at The Rogers Law Firm at 617.723.1100.