

June 2009

In This Issue

- HHS Issues Guidance on HITECH Act Technology Requirements
- False Claims Act Expanded
- OIG Approves Pay for On-Call Services to Uninsured

Services Offered by
Kroger, Gardis & Regas, LLP
Health Care Practice Group

Billing Management
Business Transactions
Compliance with Healthcare Regulations
Employment Agreements
Employment Practices
Fraud and Abuse Review
Healthcare Entity Organizations
HIPAA Compliance
Joint Ventures
Litigation
Managed Care Agreements
Management Agreements
Mergers and Acquisitions
Physician Compensation
Practice Formation/Dissolution
Sale of Practice Areas
Self Disclosure Management
Stark Law Review
www.kgrlaw.com

HHS ISSUES GUIDANCE ON HITECH ACT TECHNOLOGY REQUIREMENTS

On April 17, 2009, the U.S. Department of Health & Human Services ("HHS") issued its guidance on the technology requirements for rendering protected health information ("PHI") "unusable, unreadable, or indecipherable" to unauthorized individuals, as required by the Health Information Technology for Economic and Clinical Health ("HITECH") Act. The guidance became effective upon issuance; however, it will not apply to breaches until thirty days after HHS publishes interim final data breach notification regulations.

The HITECH Act imposes on HIPAA covered entities and their business associates breach notification requirements when "unsecured" PHI is accessed by an unauthorized party. "Unsecured" means not secured through the use of a technology or methodology that renders the information "unusable, unreadable, or indecipherable" to unauthorized individuals. However, breach notifications are not required for secured PHI.

The HHS guidance indicates that PHI may be vulnerable in the following commonly recognized data states: (a) "data in motion" - data that is moving through a network, including wireless transmissions; (b) "data at rest" - data that resides in databases, files, and other structured storage methods; (c) "data in use" - data that is in the process of being created, retrieved, updated, or deleted; or (d) "data disposed" – discarded paper records or recycled electronic media.

HHS identified two methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals: (a) encryption, which will apply only to electronic information; and (b) destruction of the PHI. If these methods are used to secure the PHI then it creates the functional equivalent of a safe harbor, whereby the

Health Line



Contact Us

<http://www.kgrlaw.com>

mjc@kgrlaw.com

lmb@kgrlaw.com

covered entity or business associate would not be required to provide notification of a data breach under the HITECH Act, notwithstanding any other federal or state notification requirements.

Encryption of "data at rest" must satisfy NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices, located on the web at the following link

<http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf>.

Valid encryption processes for "data in motion" must comply with the requirements of Federal Information Processing Standards (FIPS) 140-2, located on the web at <http://csrc.nist.gov/publications/PubsSPs.html>.

The requirements include, as appropriate, standards described in NIST Special Publications 800-52; Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs; and may include others that are FIPS 140-2 validated.

Destruction of PHI on hard copy media must render the PHI unreadable or unable to be reconstructed. PHI on electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved.

Password protecting computers, networks, and documents will not render PHI secured and in the event of a breach, the covered entity and/or business associate will be required to notify HHS and the patient(s) of the breach. Health care providers should reevaluate their HIPAA Privacy and Security programs to determine compliance with the new requirements, and should consider investing in encryption technology, if not currently used. For more information, please contact Linda Batten at lmb@kgrlaw.com or Mark Colucci at mjc@kgrlaw.com.

FALSE CLAIMS ACT EXPANDED

President Obama signed the Fraud Enforcement and Recovery Act ("FERA") on May 20, 2009. FERA is aimed at combating mortgage, financial and securities fraud, but also makes amendments to the False Claims Act ("FCA") that expands provider liability under the FCA and makes it easier for the government to investigate false claims.

Under FERA it is now a violation of the FCA if an entity "knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government." The term "obligation" includes an established duty to

Health Line



Contact Us

<http://www.kgrlaw.com>

mjc@kgrlaw.com

lmb@kgrlaw.com

repay based on the retention of any overpayment paid to an entity by the federal government. If overpayments of federal health program claims (including Medicare) are not returned a FCA action could be brought against the provider. Therefore, providers should develop and implement programs to track overpayments and return them if there is an obligation to do so. In addition, the recently instituted Recovery Audit Contractor ("RAC") audits may put providers at increased risk for discovery of such FERA violations.

FERA essentially addresses last year's Supreme Court ruling in the case of *Allison Engine Co. v. United States*, by explicitly extending the FCA to cover claims submitted to government contractors and subcontractors, including Medicare Administrative Contractors and Fiscal Intermediaries. The amendments expand whistleblower protection to any "contractor" or "agent," as opposed to the protection previously extended that was limited to employees. Furthermore, FERA provides the Attorney General with greater ability to issue Civil Investigative Demands and the government has more authority to share documents obtained through subpoena with whistleblowers.

These amendments significantly expand providers' potential liability under the FCA with minimum monetary penalties of \$5,000 per claim plus triple damages. For more information on these amendments to the FCA, please contact lmb@kgrlaw.com or mjc@kgrlaw.com.

OIG APPROVES PAY FOR ON-CALL SERVICES TO UNINSURED

On May 21 the OIG issued a new Advisory Opinion in which it addressed a growing problem in the nation's emergency rooms. The OIG concluded that a hospital plan to compensate its on-call emergency room specialists for care provided to the uninsured is "equitable," supported by a "legitimate rationale," and "would promote an obvious public benefit." Accordingly, even though the plan does not meet the four corners of the safe harbor for personal services and management contracts, the OIG determined the requisite intent to induce referrals is not present and sanctions are not warranted. for patients with complex health problems.

Under the hospital's Bylaws, all members of its medical staff are required to provide on-call coverage for the emergency department. While the hospital is paid for services rendered to the uninsured under a State program, the treating physicians are not. In addition to effectively providing services for free, the physicians

Health Line



Contact Us

<http://www.kgrlaw.com>

mjc@kgrlaw.com

lmb@kgrlaw.com

assume the liability and exposure to medical malpractice claims. The hospital has found that under such conditions it is increasingly difficult to motivate physicians to provide more than the minimum call hours necessary under the Bylaws, and has had to outsource to other hospitals.

To address the problem, the hospital developed a plan by which physicians are paid pre-established fees, at fair market value, for certain services. The valuation methodology used to determine the fees takes into account, among other things, blended fees across public, private and self payers, length of stay and likely time commitment for the services. Physicians may make a claim for the hospital payment if, among other things, the patient applies for and does not receive Medicaid coverage for the service, and the services meet certain standards (such as providing the services within 30 minutes of a request and in a face to face environment). Physicians also agree to waive all claims to third party payments if they are paid by the hospital.

The OIG expressed empathy for the plight of the hospital, while noting that such plans “create considerable risk” for fraud if physicians insist on such payments in consideration for doing business with the hospital or maintaining a relationship with the hospital. Still, the OIG noted that the key inquiry was “whether the compensation is: (i) fair market value in an arm’s-length transaction for actual and necessary items or services; and (ii) not determined in any manner that takes into account the volume or value of referrals or other business generated between the parties.” The OIG was ultimately satisfied that the plan meets that criteria.

The Advisory Opinion underscores the OIG’s appreciation for the growing problem of serving the uninsured and the key to fair market value in any compensation arrangement. For more information on compensation issues, please contact Mark Colucci at mjc@kgrlaw.com or Linda Batten at lmb@kgrlaw.com