“GAMING” ELECTRONIC HEALTH RECORDS? HHS/DOJ ISSUE A WARNING TO HOSPITALS
Hospital Associations Respond With a Request for More Guidance, Less Audits

In a letter dated September 24, 2012, the Secretary of the U.S. Department of Health and Human Services (HHS) and the U.S. Attorney General told the chief executive officers of five leading hospital associations that there are “troubling indications” that some providers are using electronic health records (EHR) to “game the system” and bill for services not rendered. More specifically, the letter claims that hospitals may be using EHR to “clone” medical records -- such as copying and pasting the same examination findings for multiple patients -- in order to “inflate what providers get paid.” In addition, Secretary Sebelius and Attorney General Holder noted that EHR could similarly tempt some providers to “upcode” the intensity of care or severity of patients’ condition as a “means to profit with no commensurate improvement in the quality of care."

Per the letter, the Centers for Medicare and Medicaid Services (CMS) is specifically initiating more extensive medical reviews to ensure that providers are coding evaluation and management [E/M] services accurately. To the extent fraud is identified, Secretary Sebelius and Attorney General Holder warned that the government will “take the appropriate steps” to pursue providers through criminal, civil or administrative enforcement proceedings, including administrative payment suspensions. Notably, as a result of the Affordable Care Act, CMS can suspend payments to a Medicare or Medicaid provider based only on a “credible allegation of fraud” as opposed to the more onerous levels of proof required for a criminal or civil proceeding. Realizing that the government cannot deter healthcare fraud by itself, Secretary Sebelius and Attorney General Holder asked the hospital associations for their help in ensuring that health information technology is not “misused or abused” as the industry phases in EHR.

Further indicating the seriousness of this issue, the American Hospital Association (AHA), one of the recipients of the HHS/Department of Justice letter, issued a reply to Secretary Sebelius and Attorney General Holder later that same day. Noting that EHR enhances a hospital’s “ability to correctly documentation and code the care a patient has received,” the AHA responded that “It’s critically important to recognize that more accurate document and coding does not necessarily equate with fraud.” The AHA informed Secretary Sebelius and Attorney General Holder that it has requested that CMS develop national guidelines for the reporting of hospital emergency department and clinic visits “11 times (starting in 2001) since the outpatient prospective payment system (OPPS) was first implemented.” Stating that “What’s needed is clearer guidance from CMS, not duplicative audits that divert much needed resources from patient care,” the AHA letter noted that “investments should be made in provider education and payment system fixes to prevent payment mistakes before they occur."

The exchange between the government and the hospital associations comes on the heels of a recent New York Times article which reported substantial increases in Medicare claims for the two highest paying categories under E/M codes used to report facility resources for clinic and emergency department visits. Characterizing
E/M coding abuses by hospitals with EHR as "widespread," the New York Times article also noted that Medicare Administrative Contractors are beginning to alert doctors of the Medicare program’s concerns over upcoding patterns for emergency department services associated with template-generated medical records.

BakerHostetler has extensive experience in advising providers on compliance with EHR, responding to government payment audits and protecting personal health information under federal privacy laws. We continue to monitor the legal issues surrounding EHR and will provide future updates as developments unfold.

For more information and advice related to regulatory and enforcement matters, please contact B. Scott McBride, smcbride@bakerlaw.com or 713.646.1390 or Gregory S. Saikin, gsaikin@bakerlaw.com or 713.646.1399. For advice with respect to electronic health records, please contact Lynn Sessions at lsessions@bakerlaw.com or 713.646.1352.

**ABOVE MARKET LEASE RESULTS IN $16.5M FINE**

HCA, Inc. has agreed to pay $16.5 million to settle allegations arising under the federal Stark Law and False Claims Act. The settlement relates to a series of financial transactions between HCA, including HCA’s Parkridge Medical Center (Parkridge) in Chattanooga, Tennessee, and Diagnostic Associates of Chattanooga (Group), a physician group acquired by HCA in 2007. In conjunction with the acquisition of the Group, Parkridge leased space in a building owned by the Group at rates which were alleged to be commercially unreasonable and excessive. The alleged misconduct also involved release of certain Group members from a separate lease obligation. The government alleged that the favorable lease terms were intended to induce the physician members of the Group to refer patients to HCA facilities.

The federal government will receive $15.7 million of the payment and the State of Tennessee will receive $807,000. Interestingly, the settlement arose as a result of a False Claims Act lawsuit filed by a real estate appraiser who will receive 18.5 percent of the payments.

This settlement illustrates the use of an alleged Stark Law violation to impose False Claims Act liability and underscores the importance of obtaining market appraisals to support lease arrangements between physicians and hospitals.

For more information, please contact Robert M. Wolin, rwolin@bakerlaw.com or 713.646.1327.

**STARK LAW ALLOWS PHYSICIANS TO BE PAID FOR DOING NOTHING**

As part of its plan to establish an open heart surgery program, St. Luke Hospitals, Inc. (St. Luke) sought a certificate of need (CON) and entered into an agreement with a group of surgeons to provide professional administrative coverage and clinical services, including provision of a full-time medical director, cardiac surgeon and on-call surgery physician, for $800,000 per year.

A competitor who opposed the CON obtained an order reversing the awarding of the CON to St. Luke, which effectively precluded St. Luke from operating an open heart surgery program. The competitor, which later merged with St. Luke, subsequently abandoned efforts to open the St. Luke heart program.

The merged hospital then ceased making payments to the physicians and sought reimbursement of all payments previously made under the agreement. St. Luke argued that the agreement required the physicians to provide open heart surgical services. None were provided, and therefore it was not required to pay. The
physicians argued that they were entitled to be paid for their "willingness" to perform surgeries. The U.S. District Court held that the plain language of the agreement entitled the physicians to payment for their willingness to perform and that there was no provision that required that services actually be rendered. Hence, providers should carefully craft language in agreements for future services to accomplish their intentions.

St. Luke’s successor next argued that its performance under the agreement was excused because the agreement was contrary to Stark Law. The hospital argued that, although the monthly payments were a flat fee, they exceeded fair market value and, therefore, must have taken into account the value or volume of referrals. However, the physicians referred only one patient during the duration of the agreement and there was no evidence whatsoever that the volume of these referrals affected the value of the hospital’s monthly payments. The court dismissed the argument based upon the evidence and concluded that the agreement did not violate Stark Law, even though no services were actually provided by the physicians.

The agreement, however, provided that if the agreement or any activities contemplated therein were deemed by either party, upon the written advice of legal counsel, to be in violation of any lawfully adopted laws, procedures, rules, regulations or policies, the agreement could be amended to comply with the laws or terminated upon 30 days written notice. Despite its finding of the agreement’s legality, the court upheld St. Luke’s successor’s notice of termination under the provision. The court concluded that the agreement requires only that a party terminate the agreement on the basis of the written legal advice of counsel. Enforcement of the provision does not require that the counsel’s advice be correct. Therefore, parties must carefully consider the terms of a right to terminate provision in an agreement to achieve their goals.

A copy of the decision, *Cardiovascular and Thoracic Surgeons Inc. v. St. Elizabeth Medical Center Inc.*, is available online.

For more information, please contact Robert M. Wolin, rwolin@bakerlaw.com or 713.646.1327.

**MASSACHUSETTS PROVIDER SETTLES WITH HHS FOR $1.5M FOR ePHI BREACH INCIDENT**

To date, HHS has entered into ten resolution agreements and imposed one civil monetary penalty related to Health Insurance Portability and Accountability Act (HIPAA) enforcement. Four resolution agreements have been triggered by a covered entity’s report of a security breach to HHS in compliance with the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

HHS’s fourth resolution agreement pertains to an April 2010 incident at Massachusetts Eye and Ear Infirmary and the Massachusetts Eye and Ear Associates, Inc. (MEEI) and MEEI’s payment of $1.5 million to settle potential violations of the HIPAA Privacy and Security Rules. MEEI also agreed to take corrective action to improve policies and procedures for safeguarding the privacy and security of their patients’ protected health information. The Corrective Action Plan (CAP), contained in the resolution agreement, can be found online. The CAP includes minimum content for policies and procedures, workforce compliance with policies and procedures, training and monitoring over a three-year period.

The settlement stems from MEEI’s April 21, 2010, reporting to HHS of the theft of an unencrypted laptop computer containing the electronic protected health information (ePHI) of 3,500 individuals – patients and research subjects, including patient names, e-mail addresses, dates of birth and medical histories. Social security numbers and financial account information were not affected by the incident. The laptop was stolen from a hospital doctor lecturing in South Korea. Immediately upon learning of the incident, MEEI remotely disabled the computer’s hard drive. HHS, upon receiving the report, initiated an investigation by the Office for Civil Rights (OCR) into MEEI’s compliance with the Privacy, Security, and Breach Notification Rules. HHS’s investigation indicated that MEEI failed to demonstrate that it conducted a thorough ongoing risk analysis regarding the confidentiality of ePHI as part of its security management process. Additionally, HHS found that MEEI lacked the following measures, policies and procedures and/or technical processes:

- Security measures to ensure the confidentiality of ePHI;
- Policies and procedures to address security incident identification, reporting and response;
- Policies and procedures for restricting access to authorized users for portable devices with access to ePHI;
- Policies and procedures governing the receipt and removal of portable devices; and
- Technical policies and procedures for restricting access to ePHI on portable devices.

OCR Director Leon Rodriguez stated in a press release regarding the settlement, "In an age when health information is stored and transported on portable devices such as laptops, tablets, and mobile phones, special attention must be paid to safeguarding the information held on these devices. This enforcement action emphasizes that compliance with the HIPAA Privacy and Security Rules must be prioritized by management and implemented throughout an organization, from top to bottom." MEEI, in a statement regarding the settlement, commented that "Given the lack of patient harm discovered in this investigation, [Massachusetts] Eye and Ear was disappointed with the size of the fine, especially since the independent specialty hospital’s annual revenue is very small compared to other much larger institutions that have received smaller fines."

Since 2008, HHS has ramped up its enforcement of the HIPAA Privacy and Security Rules. HHS’s enforcement actions have included both private and public covered entities. The evolution of HHS’s enforcement activity is as follows:

**July 16, 2008**
$100,000; resolution agreement with Providence Health & Services (stolen tapes and disks containing unencrypted ePHI of over 386,000 patients);

**January 16, 2009**
$2.25 million; resolution with CVS Pharmacy, Inc. (inappropriate disposal of PHI);

**July 27, 2010**
$1 million; resolution agreement with Rite Aid Corporation (inappropriate disposal of PHI);

**December 13, 2010**
$35,000; resolution agreement with Management Services Organization Washington, Inc. (disclosure of ePHI for marketing purposes);

**February 4, 2011**
$4.3 million; civil money penalty issued to Cignet Health of Prince George’s County, MD (denial of patient access to medical records);

**February 14, 2011**
$1 million; resolution agreement with General Hospital Corp. & Massachusetts General Physicians Organization, Inc. (loss of PHI of 192 patients);

**July 6, 2011**
$865,500; resolution agreement with the University of California at Los Angeles Health System (unauthorized employee access to ePHI);

**March 13, 2012**
$1.5 million; resolution agreement with BCBST (stolen unencrypted hard drives containing ePHI of over 1 million patients);

**April 13, 2012**
$100,000; resolution agreement with Phoenix Cardiac Surgery (public accessibility to Internet-based calendar of clinical and surgical appointments);

**June 26, 2012**
$1.7 million; resolution agreement with Alaska DHSS (stolen USB hard drive possibly containing ePHI of 501 patients); and

**September 17, 2012**
$1.5 million; resolution agreement with MEEI (stolen laptop containing ePHI of 3,500 individuals)

HHS’s last four resolution agreements have resulted from OCR investigations initiated after a covered entity’s reporting of a breach incident. From this most recent resolution agreement, it is clear that HHS will continue with OCR investigations post-breach reporting -- to ensure that a covered entity has in place policies and procedures for safeguarding PHI. Moreover, MEEI’s resolution agreement demonstrates that HHS is concerned with a covered entity’s lack of an ongoing risk assessment as to the confidentiality of ePHI. In line with the BCBST, Phoenix Cardiac Surgery and Alaska DHSS resolution agreements, a covered entity must conduct an ongoing, accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of the ePHI held by the covered entity.
SHOOT, WE FORFEITED OUR CORPORATE CHARTER – BIG HIPAA PENALTY TO INDIVIDUAL OWNERS

Uplift Medical, P.C. (Uplift) failed to provide forty-one individuals with timely access to their medical records and failed to cooperate with an HHS investigation of complaints regarding the company's noncompliance with HIPAA. Uplift argued that the medical records were not available because they were being used in a criminal hearing. As a result, HHS proposed a $4,351,600 penalty. Seems reasonable? Uplift did not request a hearing to challenge the penalty which was subsequently imposed by HHS.

Surprisingly, Uplift was no more cooperative in paying the fine than in cooperating with the investigation. As a result, HHS filed a complaint against Uplift and its owners to collect the penalty, alleging that Uplift continued operating after its corporate charter had been forfeited. HHS contended, and the court agreed, that Uplift had become a de facto partnership and its owners were therefore liable for the HIPAA civil money penalties as de facto partners. The court also held that the owners were barred from challenging the penalty for failure to exhaust their administrative remedies, by requesting a hearing and by the doctrine of res judicata.

For more information, please contact Robert M. Wolin, rwolin@bakerlaw.com or 713.646.1327.

TEXAS MEDICAID RACS ANNOUNCED

The Texas Health and Human Services Commission (HHSC) recently announced a tentative contract award for the Texas Medicaid Recovery Audit Contractor (RAC) contract to both CGI Federal, Inc. and Health Management Systems, Inc. (HMS). As noted in the April 26, 2012, issue of the Health Law Update, HHSC had previously announced a tentative award to CGI in February; however, HHSC later withdrew the announcement to request additional information from vendors, cancelled the request for proposal (RFP) and released a new RFP in June 2012. The current award is contingent upon the successful contract negotiation, and if finalized, Texas will be one of a handful of states that has awarded its RAC contract to multiple contractors.

Per the RFP, RACs will be hunting improper payments that include: (1) duplicate payments, (2) pricing errors, (3) payments for services not provided, (4) payments for noncovered services, or (5) any other errors resulting in improper payments. Claims reviewed or under review by the HHSC Office of Inspector General (OIG) or associated with an audit already underway will be excluded from the population subject to RAC audits. The RFP proposes a three-year look-back period unless a different time frame is authorized by HHSC. The RFP also contemplates that RACs will be using statistical sampling "when the RAC believes that the outcome maximizes the overpayments that will be identified."

The initial term of the contract is expected to run from about September 1, 2012, through August 31, 2015. HHSC anticipates the RACs' initial reports on potential recoveries will be submitted to HHSC approximately 3-4 months after the contract start-date.

BakerHostetler continues to follow the Medicare and Medicaid RAC program nationwide. For more information, please contact B. Scott McBride, smcbride@bakerlaw.com or 713.646.1390 or Ameena N. Ashfaq, aashfaq@bakerlaw.com or 713.646.1329.

EVENTS CALENDAR

October 9

Houston counsel Lynn Sessions will speak on "All Hands on Deck: An ERM Approach to Creating Collaboration between Compliance, Risk & Legal" at the annual meeting of the American Society for Healthcare Risk Management in Washington, D.C.
October 11
Houston counsel Gregory S. Saikin will speak on "Criminal Health Care Fraud Enforcement Update: From Audit to Appeal" before the U.S. Attorney’s Office Health Care Fraud Working Group in Tyler, Texas.

October 15-16
Houston partner Donna S. Clark will speak on "Preventing Fraud and Abuse in Your Practice" at the 2012 Texas Health Law Conference sponsored by the Texas Hospital Association in Austin, Texas.

Houston partner Susan Feigin Harris will speak on "Out of Network: Exclusion of Providers Based on Referral Patterns and Network Adequacy" at the 2012 Texas Health Law Conference sponsored by the Texas Hospital Association in Austin, Texas.

October 22
Cleveland counsel Thomas S. Campanella will speak on "The Economics of Health Care Policy" before Ohio University Osteopathic Medical Students (third year) in Columbus, Ohio.

October 23
Columbus partner Richard W. Siehl will speak on implementation of the Accountable Care Act to the Board of Directors and Faculty of the Robert C. Byrd Clinic at the West Virginia School of Osteopathic Medicine in Lewisburg, West Virginia.

October 30
Houston counsel Lynn Sessions will speak on "Lessons from Cutting Edge Transactions in Health Care and Life Sciences - HIPAA/HITECH Compliance" at the Current Issues in IP Contracting conference in Houston, Texas.

December 14
Houston counsel Lynn Sessions will speak on "Developing a Smartphone Policy for Healthcare Providers" during an audio conference sponsored by Lorman Education Services.