WINTER 2012

CORRIDORS

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

OCR Begins HIPAA Audits under the Watchful Eye of Congress: What to Expect and How to Prepare

by Elizabeth Johnson and Jessica Lewis

In November 2011, as required by the HITECH Act, the Office for Civil Rights (OCR) began auditing selected covered entities' compliance with the privacy and security provisions of HIPAA and its implementing regulations. In the near future, business associates will be eligible for audit selection as well. This article describes the current enforcement climate and provides practical steps on preparing for and responding to a HIPAA compliance audit.

Is It Getting Hot in Here? HIPAA Heats Up

The commencement of these audits is one of a series of changes that are transforming the HIPAA compliance landscape. The last two years have seen the implementation of breach notification requirements, a 60-fold increase in OCR's fining authority, increased enforcement activity with more serious repercussions for enforcement targets, and as noted, the start of OCR's compliance audits. Omnibus regulations implementing the majority of the agency's outstanding HITECH rules are anticipated shortly.

Breach notification has highlighted significant failures to secure health records, with the number of breaches reported increasing by 32% from 2010 to 2011 at an estimated cost to the health care industry of $6.5 billion. The severity of the problem has not gone unnoticed. On November 9, 2011, the Senate Judiciary Committee's Subcommittee on Privacy, Technology, and the Law convened a hearing at which its members chastised OCR for its delay in issuing final rules to implement the HITECH Act and challenged the agency to step up HIPAA enforcement activities.

Despite what appears to the regulated community as substantial enhancement of HIPAA enforcement, the Subcommittee made clear that the agency's efforts fell far short of its expectations, pointing out that, of tens of thousands of HIPAA complaints received by OCR since 2003, the agency has levied only one formal civil monetary penalty and has settled only six other cases for monetary amounts. (Of course, several of these actions reached penalties in the millions, a fact that did not assuage the Subcommittee.)

The Director of OCR, Leon Rodriguez, responded to the criticism by confirming that the agency is no longer required to provide enforcement targets with an opportunity to achieve voluntary compliance, as had been the case prior to the HITECH Act. Rodriguez stated that the agency intends to put its fining authority to good use, stating "the real frontier is in our leveraging these new, stiff penalties that we have under the HITECH statute and expanding our utilization of those penalties" to promote compliance.

The Audit Process

It is in this climate that OCR commences its first compliance audits to assess target organizations' compliance with the HIPAA Privacy, Breach Notice, and Security Rules. Of the 150 targets to be assessed in 2012, the first 20 have been notified of their selection. The audits will be conducted by OCR's contractor, KPMG LLP, which has assisted the agency in developing an audit protocol to streamline the process. In this pilot phase, the audit program functions as follows:

- OCR will inform the covered entity that it has been selected as an audit target and will request documentation of its privacy and security compliance efforts. The response is due within 10 business days.

continued on page four

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

What Hospitals and Physicians Need to Know about CMS's Proposed Rule Interpreting the Physician Payment Sunshine Act

by Wilson Hayman

Centers for Medicare & Medicaid Services (CMS) issued on December 14, 2011 its much-anticipated proposed rule interpreting the requirements of the Physician Payment Sunshine Act (Act), enacted by Congress as Section 6002 of the Patient Protection and Affordable Care Act on March 23, 2010. In its press release accompanying the proposed rule, CMS touted the Act and rule as fostering transparency which will discourage inappropriate financial relationships and give patients the information they need to evaluate their health care providers. The Act requires manufacturers of drugs, devices, biologicals, and medical supplies covered by Medicare, Medicaid, or the Children's Health Insurance Program (CHIP) to report to CMS any payments or other transfers of value they made to physicians and teaching hospitals during the preceding year. The Act also requires manufacturers and group purchasing organizations (GPOs) to report certain information regarding ownership or investment interests held by a physician or immediate family member in the manufacturer or GPO during the same time frame.

The initial reports by manufacturers and GPOs to CMS are due on March 31, 2013, for the preceding year, and on the 90th day of each calendar year thereafter. The Act requires the Secretary of the Department of Health and Human Services (Secretary) to make such information available to the public on a website no later than September 30, 2013, and on June 30 of each successive calendar year. Several states which have previously enacted similar laws drawing public attention to manufacturers' compensation to physicians have seen a reduction in such payments. CMS is currently soliciting comments concerning the proposed rule, which must be received no later than 5:00 p.m. Eastern Time on February 17, 2012.

Definitions. Under the proposed rule, the following key definitions clarify the Act's provisions and determine who and what are covered by the reporting requirements:

A "covered drug, device, biological, or medical supply" is defined as any drug, device, biological, or medical supply for which payment is available under Medicare, Medicaid, or the CHIP. In the proposed rule, CMS has clarified that this includes such items which are reimbursable either separately or as a part of a fee schedule or composite payment rate. However, covered drugs and biologicals are limited to those that require a prescription to be dispensed, not over-the-counter drugs and biologicals. Covered devices and medical supplies are limited to those that require premarket approval by or notification to the FDA. However a manufacturer that produces just one prescription drug or biological, or one device or medical supply not requiring FDA approval or notification, must report all its transfers of value to covered recipients, whether or not they are related to the covered drug, device, biological, or medical supply.

An "applicable manufacturer" is defined as an entity that is engaged in the production, preparation, propagation, compounding, or conversion of a covered drug, device, biological, or medical supply for sale or distribution in the U.S., or an entity under common ownership with such an entity which provides assistance or support to such entity with respect to those activities in the U.S.

An "applicable GPO" is defined as an entity operating in the U.S. which purchases, arranges for, or negotiates the purchase of a covered drug device, biological, or medical supply for a group of individuals or entity, not solely for use by the GPO itself.

A "physician" is defined to include doctors of medicine, osteopathy, dental surgery, dentistry, podiatry, optometry, or chiropractic licensed to practice their respective specialties in the particular state, other than employees of the applicable manufacturer. See 42 USC §§ 1320a-7h(e)(11), 1395x(r).

A "teaching hospital" is defined as any institution that received Medicare payments for Direct Graduate Medical Education, IPPS Indirect Medical Education, or Indirect Graduate Medical Education for psychiatric hospitals during the previous calendar year. Because a list of these institutions is not now publicly available, CMS proposes to publish a list of hospitals covered by the Act annually. This would include transfers of value to employees of the teaching hospital, including physicians, non-physician researchers, nurses, etc. Please note that while the Act and the implementing rule do not govern transfers of value to other, non-teaching hospitals, such hospitals could still be implicated by the Act based on payments to their physician employees or medical staff members.

Reporting Payments by Manufacturers. Physicians and teaching hospitals need to be aware of what payments or other transfers of value from manufacturers will be reported to CMS. By statute, the phrase "payments or other transfer of value" includes cash or cash equivalent, in-kind items or services and stock, stock option or any other ownership interest, dividend, profit, or other return on investment. The manufacturer must identify them as falling into one of the following categories: consulting fees, compensation for services other than consulting, honoraria, gift, entertainment, food and beverage, travel, education, research, charitable contribution, royalty or license, current or prospective ownership or investment interest, direct compensation for serving as faculty or speaker for a medical education program, grant, or any other payment or transfer of value.

Special Rules Apply to Reporting Research. A research payment may need to be reported as both a direct research payment to the hospital and an indirect research payment to the particular physician who serves as the principal investigator in a clinical trial and ultimately receives the payment. While research payments must be reported to CMS according to the same schedule as other payments, CMS (if notified by the manufacturer) will not publicly post the payment until CMS's first annual publication after the earlier of either (1) the date of approval, licensure, or clearance by the FDA, or (2) four calendar years after the date of payment. The applicable manufacturer must report to CMS each year whether a particular payment is subject to pending FDA approval and eligible for delay in publication by CMS.

Reporting Physician Investment Interests in Manufacturers or GPOs. In addition to the reporting requirement for manufacturers summarized above, both manufacturers and GPOs shall report to CMS certain information regarding any ownership or investment interest, other than in a publicly traded security or mutual fund, held by a physician or immediate family member in the manufacturer or GPO during the preceding year. The information to be reported includes the dollar amount invested, the value and terms of such investment, and any payment or transfer of value to the physician holding the interest, or transfer to another entity or individual at the request of the physician.

Exclusions to Reporting Requirement. By statute, no reporting is required for payments and other transfers of value to one physician or teaching hospital of less than $10 in 2012, unless these exceed $100 in a calendar year. These dollar amounts will be increased annually in future years by the annual percentage increase in the consumer price index. Other transfers excluded by statute are transfers of value made indirectly to a physician through a third party when the applicable manufacturer neither has actual knowledge nor acts in deliberate ignorance or reckless disregard of the identity of the physician; product samples intended for patient use but are not for sale; educational materials that directly benefit patients or are intended for patient use; the loan of a device for no more than 90 days for evaluation by the recipient; items provided under contractual warranty; transfers of anything to a physician when he or she is a patient not acting in a professional capacity; discounts and rebates; in-kind items used for the provision of charity care; an ownership or investment interest or dividend or profit distribution from a publicly traded security or mutual fund; payments to employees under a self-insured plan; transfers to non-medical professionals solely for professional services; and transfers to a physician in payment for services in a judicial or administrative proceeding. These exclusions apply to both payments or other transfers of value and ownership or investment interests.

Timetable for Submission of Information by Manufacturers and GPOs. One surprise in the proposed rule is that CMS will not require manufacturers and GPOs to start collecting data until the final regulations are issued sometime next year, though manufacturers and GPOs may begin collecting data voluntarily. Depending on when the final rule is issued, CMS is considering requiring manufacturers and GPOs to begin collecting data 90 days after publication of the final rule for the remainder of 2012, to be reported to CMS by March 31, 2013.

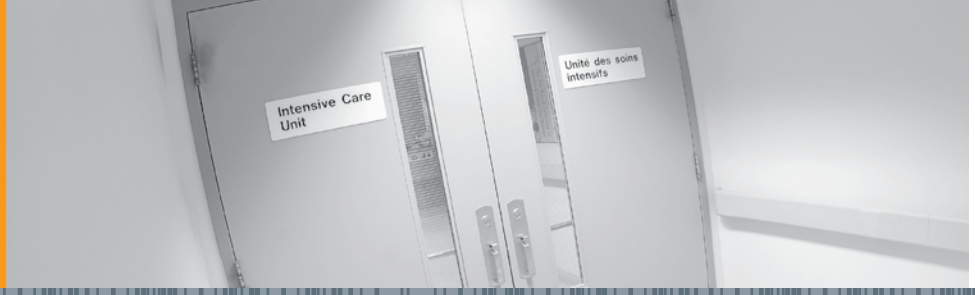
Notification of Physicians and Hospitals and Opportunity to Review Submitted Information. CMS proposes that once the data has been submitted by manufacturers and GPOs, it will notify them and the physicians and teaching hospitals when the reported information is ready for review. The manufacturers, GPOs, physicians, and teaching hospitals will all have an opportunity to review and submit corrections to the information submitted specific to that entity on a secure website for a period of at least 45 days from the date of CMS's notification before CMS makes the information available to the public. While manufacturers and GPOs will be notified through their established point of contact, physicians and teaching hospitals will be notified through CMS's LISTSERV and a posting, unless they also register with CMS to receive notification about the review processes. Registering to receive notice is recommended if a provider wishes to review the reported information. The physician must contact the reporting manufacturer or GPO to resolve any dispute regarding the reported transfer of value or investment interest, and the teaching hospital must contact the manufacturer regarding the transfer of value. If there is no agreement to resolve the matter, then CMS will make publicly available both parties' versions of the data. After the review period has expired, no person will be permitted to amend the data for that calendar year.

Availability of Reported Information to Public. CMS is required by the Act to publish by September 30, 2013, on a publicly available website, the data reported for calendar year 2012. For each year thereafter, CMS must publish the data for the preceding calendar year by June 30. CMS proposes to state on the website that publication of the payment or other transfer of value neither indicates that the payment was legitimate, nor indicates a conflict of interest or any wrongdoing. The Act also requires CMS to send annual reports to Congress and to each state summarizing the data reported.

Penalties on Manufacturers and GPOs for Failure to Report. The Act authorizes the imposition of civil monetary penalties (CMPs) in amounts between $1,000 and $10,000 on manufacturers or GPOs for each transfer of value or ownership interest which they fail to report. The total penalty for each annual submission cannot exceed $150,000. However, a manufacturer or GPO which knowingly fails to report is subject to a CMP of not less than $10,000 nor more than $100,000 for each payment or interest it fails to report, not to exceed $1,000,000 for each annual submission of information.

Effect on Hospitals and Physicians. While the Act imposes no penalties on teaching hospitals and physicians, the purpose of the Act is to shed light on the nature and extent of financial relationships and discourage inappropriate relationships and conflicts of interest. The public availability of the reported information will invite inquiring eyes to review this information. In addition to the inevitable media publicity, it is possible that investigations and prosecution of health care providers may result if inappropriate payments or relationships are revealed which arguably violate the Medicare and Medicaid Anti-Kickback Statute, the Stark Physician Self-Referral law, or similar laws. Thus, physicians and hospitals, including but not limited to teaching hospitals, should be aware of the provisions of the Act and its rules and consider tracking reportable data and retooling their compliance programs to protect themselves from the dissemination of false, damaging information.

Wilson Hayman, Editor of Corridors, *may be reached at whayman@poynerspruill.com or 919.783.1140.*



OCR Begins HIPAA Audits

CONTINUED FROM PAGE ONE

- OCR will conduct a site visit over a three-to-10-day period, interviewing personnel and observing operations. Covered entities are expected to receive 30 to 90 days' notice of the site visit.
- OCR will draft an audit report, describing the audit procedures, the findings, and the actions to be taken by the audit target in response to the findings.
- OCR will give the audit target approximately 10 business days to review the draft audit report and to provide written comments to OCR regarding concerns and corrective actions in response to the draft audit report.
- OCR will finalize the audit report within 30 business days after receipt of the audit target's response.
- If "serious compliance issues" are identified, OCR may initiate a formal compliance review. Compliance reviews can result in a formal corrective action plan and/or monetary penalties.

Preparing for and Responding to an Audit

Preparing for an audit is critical to success given the short time frame, particularly the 10-day period in which to respond to the document request. The following considerations should be evaluated immediately:

- **Documentation:** At a minimum, covered entities and business associates must have all policies and procedures required by the HIPAA Privacy, Breach Notice, and Security Rules finalized and regulator-ready. If your privacy function "owns" privacy policies and your IT function owns security policies, bring those groups together now to develop a comprehensive list of all relevant policies so they can be produced quickly. Consider other documentation that supports your compliance efforts. Are your logs of disclosures and security breaches in good order? Can you readily produce documentation supporting role-based access, systems activity review, business associate contracting, training, and other matters covered by the HIPAA rules?
- **Subject Matter Experts:** OCR will expect you to know which individuals in your organization can speak to each aspect of HIPAA implementation. Do you know who handles access requests? Who reviews access rights periodically to ensure they are correct? Who monitors system activity? What activities are logged in your systems? Who is responsible for getting appropriate contracts in place with your business associates? Who handles privacy complaints? Find these people now and ask them the kinds of questions OCR might pose.
- **Site Visits:** If you are selected for an audit, assume there will be a site visit. OCR has determined that all 150 audits in this pilot phase will result in an on site audit. Do not wait for the agency's notice of its visit to prepare.
- **Risk Analysis:** The Security Rule requires that covered entities periodically conduct a comprehensive, formal risk analysis. OCR recently released guidance on conducting such an analysis. The results of that analysis will be among the documents the agency can (and is very likely to) request for review. If you have not conducted a risk analysis in the last 12 months, do so now. Upon completion, evaluate the results and determine how best to mitigate or manage each risk identified (an activity also required by the Security Rule). Document the entire process.
- **Breach Notice and Incident Response:** By now, your organization should have implemented a written incident response plan that reflects the requirements of both the Breach Notice Rule and the Security Rule. Ideally, your organization will also conduct a trial run of its response plan and adjust the procedure as needed in light of the results.
- **Evaluate Compliance:** Your organization is required to periodically evaluate the effectiveness of its compliance program, including the evaluating accommodations to the recent legal changes brought about by the HITECH Act and implementing regulations.
- **Training:** If you have not consistently or recently trained employees, now is a good time for a refresher. Maintain documentation evidencing that every relevant employee has been trained.
- **Business Associates:** If you have not identified all of your vendors that handle protected health information, now is an excellent time to do so. Negotiate business associate agreements with all such vendors.
- **Timely Response:** Make sure that the appropriate people will receive, in a timely manner, OCR's written notice of its intent to audit. Do not let the notice sit in someone's inbox while he or she is on vacation for a week, cutting your response time in half.
- **Influencing the Audit Report:** The agency provides covered entities with an opportunity to respond to the draft audit report. In our experience working with HIPAA assessors, they will be very responsive to constructive feedback, including presentation of new facts, legal arguments regarding the scope and application of the rules, and justification of your approach to implementation based on the unique position of your organization. When you receive the draft audit report, formulate a response to any findings that you believe were unfair or inaccurate.
- **Next Steps:** Once the audit is over, be sure to take any compliance steps the agency has mandated, and seriously consider taking any it has suggested. Failure to demonstrate reasonable progress on the audit findings, particularly if brought to light by a reportable security breach, will almost certainly result in swift enforcement action by the agency.

Whether or not your organization is ever selected for an audit, the preparatory steps described above will enhance your organization's compliance posture. In a time when fines surpass the million-dollar mark and a security breach lurks around every corner, undertaking that work will pay dividends even if your organization avoids an audit. Of course, if you do find yourself among the lucky first 150 audit targets, you'll certainly be glad you took the time to prepare in advance.

Elizabeth Johnson may be reached at ejohnson@poynerspruill.com or 919.783.2971. Jessica Lewis may be reached at jlewis@poynerspruill.com or 919.783.2941.

Over 3 Billion Reasons to Know the Government's Plan

By Kim Licata

Civil cases involving fraud against the government continue to be lucrative for the federal government. For the second year in a row, the federal Department of Justice recovered over $3 billion relying on the federal False Claims Act (and its treble damages provision). In fiscal year 2011, $2.4 billion of the $3 billion recovery came from alleged fraud against federal health care programs, such as Medicare and Medicaid that were paid by health care providers and suppliers. Anticipate continued aggressive enforcement against providers in 2012, and take the time now to review your compliance with health care laws and regulations.

How can you protect yourself? A myriad of laws and regulations affect hospitals, and you can best protect your business by following these three steps. First, know what the government is interested in. Second, consider which of the government's concerns apply to your hospital, assess how your hospital handles these concerns in practice, and develop a plan to address vulnerabilities. Third, seek appropriate counsel if you determine that your current practices may subject your hospital to governmental scrutiny.

How do you find out what the government is reviewing? Review the work plan issued by the lawyers for the federal Department of Health and Human Services (HHS) and the Office of Inspector General (OIG). This publicly available plan identifies the arrangements or activities that the OIG believes are sensitive to fraud and abuse. Each year, the OIG Work Plan includes some initiatives from the prior year(s) along with new concerns. The Work Plan identifies 23 initiatives focused on hospitals, but only six are new this year. The new initiatives include (1) accuracy of present-on-admission indicators submitted on Medicare claims, (2) review of Medicare inpatient and outpatient payments to acute care hospitals through focused reviews of claims, (3) acute-care hospital inpatient transfers to inpatient hospice care with an eye toward financial relationships/ownership between the two providers, (4) Medicare outpatient dental claims, (5) appropriateness of admissions to inpatient rehabilitation facilities, and (6) profiling of critical access hospitals as to their structure and types of services provided.

Several existing initiatives were added through the Affordable Care Act (same day admissions, reliability of hospital-reported quality measure data); others have been ongoing for several years.

Remember that the government is armed with new, expansive powers under health care reform and has every incentive to review claims for overpayments. The government will use data mining, sampling, and other comprehensive methods to identify risky claims and submitters of these claims. Assess your practices now to make sure your facility isn't contributing to a record-breaking fraud recovery next year.

Kim Licata may be reached at klicata@poynerspruill.com or 919.783.2949.

CMCS Launches New Medicaid Website

by Chris Brewer

The Center for Medicaid and the Children's Health Insurance Program (CHIP) Services (CMCS) now has an official government website designed to make more information and resources available about these programs. The purpose of Medicaid.gov (http://www.medicaid.gov) is to provide easy access to current events, announcements, and policy issues to all persons interested in the Medicaid and CHIP health coverage programs. Medicaid.gov topics include federal policy guidance, state-specific program data, and Affordable Care Act implementation updates. There is also a section devoted entirely to pending and approved waivers. The site also has a section with enhanced search capabilities for consumers. Medicaid.gov has helpful links to http://www.healthcare.gov/ and http://www.insurekidsnow.gov/ which provide additional information about health coverage options.

Chris Brewer may be reached at cbrewer@poynerspruill.com or 919.783.2891.

North Carolina to Join Ranks of States Requiring Employers to Enroll in E-Verify

by Jennifer Parser

The North Carolina Legislature passed a bill that will gradually require all private employers with more than 25 employees to use the federal online E-Verify program to verify the employment authorization of newly hired employees. The bill, HB 36, was passed on June 18, 2011, and was signed into law by Governor Beverly Perdue on June 23, 2011, as Session Law 2011-263. E-Verify is a free Internet-based system that allows employers to determine employment authorization by checking an employee's documentation against Department of Homeland Security and Social Security Administration databases. Employers can enroll in E-Verify at https://e-verify.uscis.gov/enroll/.

This new E-Verify law required North Carolina counties and cities to register and participate in E-Verify by October 1, 2011. Private sector employers' participation in E-Verify is being phased in more slowly, according to the employer's size:

- Employers with 500 or more employees will be required to participate by October 1, 2012;
- Employers with 100 or more employees will be required to participate by January 1, 2013; and
- Employers with 25 or more employees will be required to participate by July 1, 2013.

Businesses will not be required to verify the employment eligibility of current employees unless the employer has been awarded a federal contract on or after September 8, 2009, that contains the Federal Acquisition Regulation (FAR) E-Verify clause. Also, industries that hire agricultural workers for 90 days or less in a 12-month period are exempt from using E-Verify. Civil penalties for violations of North Carolina's E-Verify law are to be assessed by the NC Commissioner of Labor and will range from $1,000 to $10,000. Employers with more than 25 employees would do well to visit the above mentioned E-Verify website to acquaint themselves with E-Verify and attendant enrollment procedures well before enrollment is required.

The federal government has recently added E-Verify Self-Check which permits an employee or prospective employee to check his or her employment eligibility, just as an employer would when it uses E-Verify. E-Verify Self-Check also provides information to the employee on how to correct any problems. The E-Verify Self-Check website is https://selfcheck.uscis.gov/SelfCheckUI/start.html. E-Verify Self-Check is being phased in slowly on a national basis and is currently offered to individuals who maintain addresses in 21 states. North Carolina does not yet have E-Verify Self-Check, although neighboring Virginia and South Carolina do.

For updates on immigration news of interest, follow Jennifer Parser @immigrationgal on Twitter.

Jennifer Parser practices in the areas of immigration, employment, and international law. In her practice, she assists clients with a variety of immigration and employment issues. Jennifer may be reached at jparser@poynerspruill.com or 919.783.2955.

POYNER SPRUILL IS GOING GREEN **In an effort to be more environmentally conscious, we also issue Corridors by email. To sign up for an email subscription to Corridors, please send an email request to alerts@poynerspruill.com with Corridors in the subject line. Save a tree!**

p.s.