JANUARY 2016

CORRIDORS

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

Final Stark Rule Changes Adopt New Exceptions For Hospitals and Significant Clarifications

by Wilson Hayman

In the Medicare Fee Schedule Final Rule with Comment Period for calendar year 2016, the Centers for Medicare & Medicaid Services (CMS) adopted two new exceptions to the Stark physician self-referral law affecting hospitals, effective January 1, 2016, and made certain other significant changes. 80 Fed. Reg. 70885, 71300 (Nov. 16, 2015). A proposed rule including many of these revisions was first published in the Federal Register on July 15, 2015, and was the subject of an article in our September 2015 issue of *Corridors*. This article will summarize the changes to the Stark law in the final rule and delineate some of CMS's changes from the proposed rule. Most should be welcomed as lessening the risk for North Carolina hospitals and physicians of committing minor, technical violations of the Stark law.

New Exception for Hospital Recruitment of Nonphysician Practitioners Includes Mental Health Practitioners

Changes from Proposed Rule. The final rule changed the proposed recruitment exception permitting hospitals, federally qualified health centers and rural health clinics to provide remuneration to a physician for the recruitment of non-physician practitioners (NPPs), to be codified at 42 CFR § 411.357(x). In recognition of the widespread shortage of mental health professionals, CMS in the final rule broadened the services to include not only primary care but also mental health services. The final rule expands the definition of NPP for the new exception to include clinical social workers and clinical psychologists, besides the physician assistants, nurse practitioners, clinical nurse specialists, and certified nurse midwives covered by the proposed rule. Other changes include that the NPP need not be employed by the physician but may be an independent contractor. For an independent contractor under this exception, the contractual relationship for services must be directly between the physician (or physician organization) and the NPP. Without physician involvement, Stark is not implicated; CMS noted that a hospital's recruitment payments made directly to an NPP triggers the Stark law only if the NPP serves as a conduit for physician referrals or is an immediate family member of a referring physician.

Requirements of Final Rule on Recruitment of NPPs

The exception for assistance to a physician to compensate (as an employee or contractor) an NPP to furnish patient care services requires that (1) the arrangement is set out in writing and signed by the hospital, the physician and the NPP; (2) the arrangement is not conditioned on the physician's or NPP's referrals to the hospital; (3) the remuneration from the hospital does not exceed 50 percent of the actual compensation, signing bonus and benefits paid by the physician to the NPP during a period not to exceed the first two consecutive years of the compensation arrangement and is not determined in a manner that considers the volume or value of any referrals by the physician or the NPP (or any physician or NPP in the physician group practice) or other business generated by the parties; (4) the compensation, signing bonus and benefits paid by the physician do not exceed fair market value for the patient care services furnished by the NPP to the practice; (5) the NPP has not, within one year of commencing the compensation arrangement with the physician, practiced in the geographic area served by the hospital or been employed or engaged to provide patient care services by a physician or physician group with a medical practice site in the hospital's geographic area, whether or not the NPP provided services in that geographic area; (6) substantially all (i.e., 75 percent) of the services provided by the NPP to the physician's patients are primary care or mental health care services; (7) the physician does not impose practice restrictions that unreasonably restrict the NPP's

continued on page two

Final Stark Rule Changes...

CONTINUED FROM PAGE ONE

ability to provide patient care services in the hospital's geographic area; and (8) the arrangement does not violate the Anti-Kickback Statute or other federal or state law governing billing or claims submission. This exception may be used by a hospital only once every three years regarding the same referring physician, unless the NPP is replacing an NPP who terminated his or her employment or contract to provide patient care services with the physician, and the remuneration is provided within two consecutive years measured from the commencement of the arrangement with the NPP being replaced. See 42 CFR §411.357(y).

New Exception for Timeshare Arrangements

The current Stark exception for office lease arrangements does not permit timeshare leasing arrangements in which a physician does not receive a possessory interest in property as in a true lease but pays the lessor for the periodic right to use office space exclusively on a turnkey basis, including support personnel, waiting area, furnishings, equipment, and supplies. Such arrangements are common in rural areas where a hospital or physician practice makes space and staff available to a visiting physician. This is often structured as the owner's grant of a license or privilege to the visiting physician for the property at specified times, without conveying dominion or control over the premises as in a true lease. The final rule made several relatively minor changes from the proposed rule. It creates a new exception codified at 42 CFR § 411.357(y) permitting timeshare arrangements that meet these criteria: (1) the arrangement is set out in writing, signed by the parties, and specifies the premises, equipment, personnel, supplies, and services covered; (2) the arrangement is between a physician or physician group as licensee and either a hospital or another physician organization (of which the licensee physician is not an employee, owner or member) as licensor; (3) the licensed premises, equipment, personnel, items, supplies, and services provided are used predominantly for evaluation and management services for patients and on the same schedule; (4) the licensed equipment is in the office suite where the evaluation and management services are furnished, is not used to furnish DHS other than those incidental to the evaluation and management services furnished, and does not include advanced imaging, radiation therapy or clinical or pathology lab equipment; (5) the arrangement is not conditioned on the physician licensee's referral of patients; (6) the compensation is set in advance, consistent with fair market value and neither (a) determined in a manner that considers the volume or value of referrals or other business generated between the parties, nor (b) based on a percentage of revenue or per-unit of service, other than time-based, that reflects the services provided to patients referred by the licensee physician; (7) the arrangement would be commercially reasonable even absent referrals between the parties; (8) the arrangement does not violate the Anti-Kickback Statute or any other federal or state law governing billing or claims submission; and (9) the arrangement does not convey a possessory leasehold interest in the office space that is the subject of the arrangement.

Summary of Other Changes to Stark Rule

The final rule adopted, among others, these additional changes to the Stark rule:

Writing and Signature Requirements. The final rule clarifies that while the terms of compensation arrangements such as leases and personal service arrangements must be sufficiently documented, these exceptions do not require them to be documented by a single, formal contract or any other particular kind of writing. Therefore CMS has replaced the terms agreement and contract in those exceptions with arrangement. See 42 CFR §§ 411.354(d), 411.357(a), (b), (d).

For compensation arrangement exceptions that require the parties' signatures, the final rule gives the parties 90 days from the date the compensation arrangement became noncompliant, whether or not their failure to obtain the signatures was inadvertent. See 42 CFR § 411.353(g).

Term Requirements and Holdover Leases. The final rule provides that an arrangement for the lease of office space or equipment or for personal services, which can be documented to have lasted for at least one year (or which was terminated during the first year and the parties did not enter a new arrangement for the same space, equipment or service), satisfies the requirement of a one-year term. See 42 CFR §§ 411.357(a), (b), (d). The parties need not have an agreement with a term of at least one year.

The final rule provides that holdover leases for an unlimited period comply with the Stark rule if the arrangements meet the applicable exception when the arrangement expired and continue to meet requirements, and the holdover is on the same terms and conditions as the prior arrangement. See 42 CFR §§ 411.354(d), 411.357(a), (b), (d).

Definition of Stand in the Shoes. CMS has revised 42 CFR § 411.354(c)(3)(i) to clarify that while only physicians who "stand in the shoes" of their physician organization are parties to the arrangement for signature, all physicians in the physician organization are parties to the arrangement for all other purposes, including whether the compensation with the hospital considers the volume or value of referrals or other business generated by the physicians.

Wilson Hayman's practice focuses on health care, appellate, civil, and administrative law and is editor of *Corridors*. He may be reached at 919.783.1140 or whayman@poynerspruill.com.

CMS Initiatives Target Quality & Care Improvement

by David Broyles and Iain Stauffer

Like it or not, the Centers for Medicare & Medicaid Services (CMS) is showing a strong commitment to moving forward with its focus on hospitals' quality and care improvement as the basis for payment. In November, CMS published the final rule for the Comprehensive Care for Joint Replacement (CJR) model (November 16, 2015), as well as a proposed rule that would revise the discharge planning conditions of participation (CoPs) for hospitals, including critical access hospitals.

CJR Final Rule

Under the CJR model, participation will be mandatory, effective April 1, 2016, for almost 800 hospitals across the country, divided into 67 geographic areas. North Carolina has four geographic areas affected: Asheville, Charlotte-Concord-Gastonia, Durham-Chapel Hill, and Greenville. A listing of the participant hospitals in these four geographic areas can be found at https://innovation.cms.gov/initiatives/cjr. Participant hospitals will be held financially accountable for the quality and cost of care provided to Medicare fee-for-service beneficiaries for lower-extremity joint replacement procedures and recovery, including all hip and knee replacement surgeries, for the 90-day period following hospital discharge (episode). Lower-extremity joint replacements are the most commonly performed Medicare inpatient surgery, with predictions showing continued growth in utilization. The quality and cost of care for an inpatient stay that results in a Diagnostic-Related Group (DRG) of 469 or 470, along with all related care provided during the episode, will be measured and adjusted using a retroactive bundled payment. The payment model and phases of the CJR model will extend for five performance years, concluding on December 31, 2020.

Responding to nearly 400 comments filed following the publication of the proposed rule, CMS delayed the initial start date from January 1, 2016, to April 1, 2016, as well as implemented certain target pricing on the DRGs affected, a weighted methodology for quality and patient satisfaction in determining incentive payments, and stop-loss and stop-gain limits to protect both hospitals and CMS. Waivers for certain fraud and abuse authorities were issued jointly by CMS and the United States Department of Health and Human Services (HHS) Office of Inspector General (OIG) concurrently with the CJR final rule. Those waivers, which include waivers for specified arrangements involving comprehensive care for hip and knee joint replacement model participants, can be found at https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/Fraud-and-Abuse-Waivers.html.

Participant hospitals are encouraged to enter into financial arrangements in the form of collaborator agreements and/or sharing arrangements with post-acute care (PAC) providers and others related to gainsharing payments for CJR, distributions of payments from a group practice following payment by a hospital, and certain patient engagement incentives made to beneficiaries. All of these payments align with CMS's shift in focus to incentivize hospitals and PAC providers to work together, with the goal of improving quality of care provded to patients.

For additional information, please see the CMS Fact Sheet – CJR Model at https://www.cms.gov/Newsroom/MediaReleaseDatabase/Fact-sheets/2015-Fact-sheets-items/2015-11-16.html and the CJR Final Rule Text found in the Federal Register at https://www.federalregister.gov/articles/2015/11/24/2015-29438/medicare-program-comprehensive-care-for-joint-replacement-payment-model-for-acute-care-hospitals.

Discharge Planning Requirements Proposed Rule

In the discharge planning CoPs proposed rule issued by CMS on November 3, 2015, CMS is clearly focusing on improving health outcomes and reducing health care costs by decreasing patient complications and avoidable hospital readmissions with more robust discharge planning requirements. Consistent with the CJR final rule summarized above, CMS intends for the new requirements to increase communication between providers, patients, and families/caregivers in the discharge planning process by incorporating patient goals and utilizing quality and resource-use data to help patients select their PAC provider. The proposed CoPs rule at 42 C.F.R. § 482.43 recommends six new standards, which contain more specific requirements with necessary, precise measures that must be undertaken by a hospital prior to a patient's discharge or transfer to a PAC setting. All these measures require the discharge plans to

continued on page five

Who's Going Under the Bus? Federal Policy on Individual Responsibility for Corporate Wrongdoing

by Steve Shaber

In a wake-up call to health care corporate officers and managers, Deputy Attorney General Sally Yates earlier this fall announced a new, tougher U.S. Department of Justice policy regarding individual responsibility for corporate wrongdoing, both civil and criminal. DOJ needs this new policy, she said, because it is so difficult to identify the person or group of people in a large company who knew they were doing something wrong and had the intent to be legally culpable.

When a company has up-coded services and overcharged its payors, it may be easy to show that the company did something seriously wrong. The codes and bills are all recorded on the servers, as are all the clinical services rendered. Comparing one to the other, the codes may be wrong and the overpayments indisputable.

But the company's liability raises questions: Who knew what was happening, when did they know it, and did they know it was wrong? Typically, the clinicians will say they had no role in the coding, the billing staff will say they were trained to code things the way they did, the trainers will say they relied on information from headquarters, while corporate officers will say they hired consultants to tell the company what to do. And so it goes because – as we all know – the search for someone else to blame is never fruitless.

The Key Change

In the past, in cases like the example above, the federal government has been inclined to do what was easier and go after the company without insisting on finding the people who made the improper decisions for the corporation. The government would even let the company cooperate with the investigation and would lessen its financial penalties.

But no more. The Department of Justice has made companies tell all. In the words of Deputy Attorney General Yates, "[i]f a company wants any consideration for its cooperation, it must *give up the individuals*, no matter where they are in the company." Someone – the right someone – has to go under the bus, or the corporation will suffer.

Important Elements of the New Federal Policy

The key statement in the new federal policy, the one which Deputy Attorney General Yates summed up when she said "give up the individuals," is this: "In order for a company to receive any credit for cooperation... the company must completely disclose to the Department [of Justice] all relevant facts about individual misconduct. Companies cannot pick and choose."

In some other key items, the federal government also said:

- It will focus its investigations on individuals "from the very beginning."
- The settlement with the corporation will seldom, if ever, provide any civil or criminal protection to individuals.
- The government will no longer be willing to forgo action against an individual simply because the individual cannot pay back to the government an appreciable amount of money.

Taken together, these factors demonstrate the DOJ's new emphasis on punishment and restitution as well as deterrence.

Business Tip

This new policy may give new power to corporate compliance officers. In the past, the compliance officer (CO) could tell management it might be possible to protect both the company and the responsible individuals, so management could ask the CO to do both. Under the new policy, however, only full disclosure of "all relevant facts about individual misconduct" will help the company, so the CO is less likely to face conflicting instructions.

Legal Tip

All concerned should remember that the company's lawyers represent the company and not any of its directors, officers, or employees. The job of those lawyers is to help the company decide whether it is in the company's interest to cooperate, i.e., turning over the individuals

to the government to get a better deal for the company itself. Any officers or employees suspected of individual wrongdoing cannot rely on company counsel for advice; they must have their own lawyers, and they need them initially. In some instances, the company or its insurers will pay separate lawyers to represent the individuals caught up in the investigation, but separate counsel will usually be necessary from early on. The only thing more uncomfortable and dangerous than sorting out these conflicts at the start of an investigation is to do it halfway through the process.

Conclusion

Ben Franklin may have said that he and his patriot friends should "all hang together" against the Crown, or else they would "assuredly all hang separately." This warning may still apply when the government comes to investigate small companies, such as the three-doctor practice or the independent pharmacy. On the other hand, when a company is large enough to have multiple locations, various unrelated lines of business, a distant corporate headquarters, or an independent board of directors, people could cooperate with the investigation because their welfare depends on the company's well-being. But there will also be people, such as those whose decisions led to the investigation, with interests that are adverse to the company's. More than ever before, the DOJ intends to find and hold the responsible people accountable by any means necessary, including the DOJ's pitting one group of people against another.

For more information, see "Individual Accountability for Corporate Wrongdoing," U.S. Department of Justice, Office of the Deputy Attorney General (September 9, 2015).

Steve Shaber has spent his entire career in health law – first with the North Carolina Attorney General's Office and, since 1985, in private practice. His clients range from large hospitals to sole practitioners. Steve may be reached at sshaber@poynerspruill.com or 919.783.2906.

CMS Initiatives...

Continued from page three

focus on specific patient-centered goals, preferences and needs. Interested stakeholders may file comments until January 3, 2016.

The CMS News Release Information concerning the proposed CoPs rule can be found at https://www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2015-Press-releases-items/2015-10-29.html, and the CoPs Proposed Rule Text has been printed in the Federal Register at https://www.federalregister.gov/articles/2015/11/03/2015-27840/medicare-and-medicaid-programs-revisions-to-requirements-for-discharge-planning-for-hospitals.

These particular rules, along with other ongoing CMS payment initiatives, should put hospitals on alert that CMS is determined to utilize quality and resource-use data to improve health outcomes and reduce health care costs in the hospital and PAC settings. Whether or not your hospital facility is named as part of any current CMS mandatory program, all signs point to CMS continuing to expand its focus on quality-based initiatives. Hospital leadership and experienced legal counsel should closely review all related policies, procedures, facility practices, and arrangements to ensure full, continued compliance.

David Broyles focuses his practice on representing health care providers, with an emphasis on Certificate of Need, health care licensure and certification, reimbursement, regulatory, and operations issues. David may be reached at dbroyles@poynerspruill.com or 919.783.2923.

Iain Stauffer's practice focuses on advising and representing health care providers in Medicare and Medicaid reimbursement, enrollment, compliance, litigation, and regulatory issues. He may be reached at istauffer@poynerspruill.com or 919.783.2982.

Proposed CON and Reporting Rules in the Works at DHHS

by Todd Hemphill

The N.C. Department of Health and Human Services (the Department) has recently proposed changes to the rules governing health service facilities, including hospitals. The Department's Healthcare Planning and Certificate of Need Section (the CON Section) has proposed eliminating several rules related to information required for CON applications, while the Medical Care Commission has proposed temporary rules changing certain reporting requirements for hospitals and ambulatory surgical facilities in response to recent legislation. Each of these developments is discussed below.

Proposed Repeal of Certain CON Rules

The rules promulgated by the CON Section contain provisions requiring CON applicants to provide multiple forms of information with the application. These rules include requirements related to a facility's physical plant, support services, staffing and staff training, and other operational issues. Many services covered are those provided by hospitals, including rules related to the development or addition of acute care beds, psychiatric beds, intensive care services, neonatal services, open heart surgery services, burn intensive care services, rehabilitation services, operating rooms, GI endoscopy procedure rooms, cardiac catheterization and cardiac angioplasty equipment, radiation therapy equipment, CT scanners, MRI scanners, gamma knife, PET scanners, major medical equipment, lithotriptor equipment, bone marrow transplantation, and solid organ transplantation.

The CON Section has proposed eliminating all of these rules, leaving intact only definitional rules and the performance standards (which require the applicant to provide historical and future utilization data to demonstrate need for the service proposed). The proposed changes can be found in the North Carolina Register at pp. 890-894.

In its comment to the proposed rules, the CON Section explains the proposed repeal:

- To the extent the information requested in these rules is needed to determine conformity to the review criteria in G.S. 131E-183(a), it can be obtained through the CON application forms authorized by G.S. 131E-182(b), which need not be promulgated as rules. Therefore, the rules proposed to be repealed are not needed.
- Some of these rules are too vague and many are outdated, with effective dates as far back as 1983.
- The rules also place an unnecessary burden on applicants and increase the complexity of litigation, which increases costs for both the CON Section and applicants.

During a public hearing held November 20, 2015, Martha Frisone, assistant chief of the CON Section, advised that to date, she had received no objections to the proposed rule changes. None were expressed at the public hearing. Ms. Frisone also advised that if there are no objections to the rules and they are approved at the Rules Review Commission's January 2016 meeting, they would become effective on February 1, 2016.

Ms. Frisone advised that the CON Section also intends to update the CON application forms in use during the next year. The CON Section intends for the revised forms to ask questions based on each of the statutory review criteria in G.S. 131E-183(a). The new form has already been created for CON applications for dialysis services. Those forms were created with the input of the major dialysis providers in the state. The CON Section has begun preparing updated application forms for acute care services and medical equipment, which they hope to have finished after the middle of 2016. As with the dialysis forms, the CON

Section intends to seek the input of the major stakeholders for acute care services prior to finalizing these forms.

Finally, the CON Section intends to revisit the performance standard rules, to determine whether any are outdated and need to be revised.

Proposed Revisions to Hospital and Ambulatory Surgical Facility Reporting Requirements

In the past decade, several states have enacted health care price transparency or disclosure legislation as a strategy for containing health care costs, requiring providers to disclose the costs associated with certain services, either directly to patients or through reporting requirements to state agencies. One major driver of these laws has been the increase in high-deductible health insurance plans, both individually and in employer-based group plans. Because consumers increasingly must pay more out of pocket for health care services, requiring public disclosure of this information provides consumers with tools to make better informed decisions regarding the price they pay for health care, potentially reducing overall health care costs.

In 2013, the North Carolina General Assembly enacted the Health Care Cost Reduction and Transparency Act (the Act), imposing reporting requirements regarding charges and reimbursement on hospitals for the 100 most frequently reported admissions by DRG for inpatients, and on hospitals and ambulatory surgical facilities (ASFs) regarding the 20 most common ambulatory surgical procedures and outpatient imaging procedures. These changes, codified in G.S. 131E-214.11, et seq., required this information be reported quarterly to the Department. The statute also required the Medical Care Commission to promulgate rules ensuring that this information would be reported in a uniform manner. In response, the Medical Care Commission promulgated temporary rules on December 31, 2014. and permanent rules on September 30, 2015, incorporating these requirements.

Near the end of the 2015 session, the General Assembly inserted a provision in the budget modifying the reporting requirements in the Act by requiring *annual*, rather than *quarterly*, reporting of this data. See S.L. 2015-241 (H97) [http://www.ncleg.net/Sessions/2015/Bills/House/PDF/H97v9.pdf], pp. 139-141. In response, the Medical Care Commission has announced its intent to promulgate temporary rules to incorporate these proposed changes. These changes, codified in 10A N.C.A.C. 13B.2102 and 10A N.C.A.C. 13C.0206, require hospitals and ASFs to file annual reports by January 1 of each year, commencing with the reporting period ending September 30, 2015.

So far, we have not determined the General Assembly's reasons for this change. Maybe the legislators who wanted this data felt that annual information would be more useful. At any rate, this statutory and rule change will make it simpler for hospitals and ASFs to provide this information.

The proposed effective date of the temporary rules is February 26, 2016. More information regarding these proposed rule changes can be found at the Department's web site at http://www2.ncdhhs.gov/dhsr/rules/temptransparency2015.html.

Todd Hemphill's practice focuses on health care strategic planning issues, assisting clients in developing health care development strategies under the Certificate of Need law, negotiating health care transactions, litigating Certificate of Need awards and denials, licensure and certification issues, including appeals challenging certification and licensure survey decisions and penalties. Todd may be reached at 919.783.2958 or themphill@poynerspruill.com.

What They Mean for Phase 2 Audit Preparation and Compliance Planning

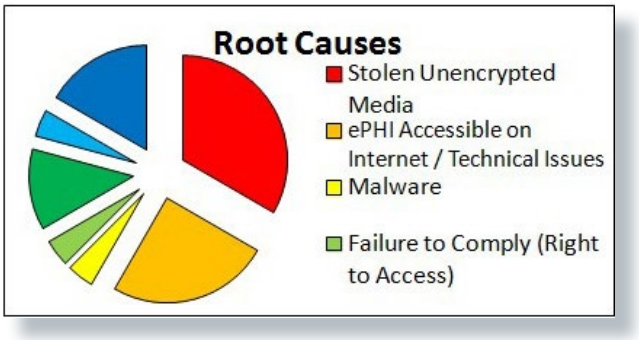
by Tara Cho

The Office of Civil Rights (OCR) recently announced plans to begin the next round of its HIPAA audit program in early 2016. In comments responding to two reports issued by the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services on September 29, 2015, OCR announced that it will begin Phase 2 of the HIPAA audits early next year. Consistent with prior descriptions of the Phase 2 audits, OCR stated in its recent response to OIG that the audits would include a combination of desk audits and on-site audits, will involve both covered entities and business associates, and will target specific common areas of noncompliance. OCR Director Jocelyn Samuels previously indicated that in the Phase 2 desk audits, covered entities and business associates will have two weeks to upload applicable HIPAA policies and procedures to a portal for OCR auditors to review. This remote audit approach will not allow for additional clarifications or discussion between the auditor and entity; therefore, policies and procedures must be accurate, complete and ready to upload.

In addition to being prepared for the Phase 2 audits, privacy and information security requirements impact the entire scope of a provider's operations and are key components of a comprehensive compliance strategy. Ensuring the privacy and security of patients' Protected Health Information (PHI) is especially important as regulatory oversight increases for hospice providers, with efforts to hold those providers more accountable for their quality of care.

Trends from past HIPAA enforcement actions by OCR can help providers focus their compliance planning, identify potential vulnerabilities and be best prepared should they be the subject of an OCR audit. Reviewing the root causes of these enforcement actions can point to valuable lessons learned. The most common root cause for enforcement actions from 2008 to 2014 related to stolen, unencrypted media such as laptops or USB drives. This category was followed by a number of enforcement actions stemming from technical issues or implementation errors that made Electronic Protected Health Information (ePHI) accessible to the public on the Internet or subject to other unauthorized access. There were also several actions related to the improper disposal of hard copy PHI and failure to comply with requirements of the Privacy Rule, such as providing patients a right to access their PHI or inappropriate uses and disclosures by staff or other authorized users.

Most of these enforcement actions resulted from investigations following breach notification by the covered entity or individual complaints to OCR. Therefore, in addition to the high costs of settlement amounts and required corrective action plans that result from regulatory enforcement actions such as these, providers must also consider the costs associated with a breach, including expenses involved in actual breach notification, investigation and cyber forensics costs, legal fees, and reputational damage, when planning a risk management strategy. It is also notable that enforcement actions span various types of entities including nonprofits, large retail pharmacies, regional medical centers, large health systems, and government agencies. Surprisingly, although different entities may share the same root cause for the incident that triggered investigation and enforcement, there seems to be a correlation between the entity's ability to pay and the size of the settlement. For example, a retail pharmacy paid $2.25 million for inappropriate disposal of PHI in a store dumpster, while a smaller health system paid



$800,000 for leaving 71 boxes of paper medical records in a physician's driveway accessible to the public. The risks to the hard copy PHI were very similar, but the settlement amounts reflect the size and capabilities of the different entities. Regardless of size and operations, entities should be aware of their regulatory obligations and the threats to their networks, systems, and data.

So, what can covered entities and business associates learn from these enforcement actions?

- **Encrypt! Encrypt! Encrypt!** Although encryption is not a mandatory specification in the HIPAA Security Rule, encryption can greatly mitigate the potential risks that result from theft or loss of a portable device (e.g., mobile phone or laptop) or removable media (e.g., CD or USB drive). Encryption can also be a safe harbor from breach reporting requirements, and OCR has repeatedly noted the importance of applying encryption whenever possible.
- **Risk Analyses.** Conduct ongoing risk analyses of systems, networks, equipment, and other repositories or access points to ePHI. Implement remediation plans and update policies and procedures to address critical risks identified during such risk analyses.
- **Device Management.** Don't sell, retire or reissue computers, portable devices, or even leased copiers or scanners without securely wiping all content. Implement appropriate policies and controls around mobile devices, particularly personal mobile devices used for work.
- **Hardcopy PHI.** Do not underestimate or forget the security threats to nonelectronic PHI and the associated requirements. Maintain policies and procedures to implement Privacy Rule requirements and to control the security and disposal of hard copy PHI.
- **Training.** Train employees and monitor adherence to HIPAA policies and procedures, including permissible uses and disclosures and incident reporting. In addition, educate employees with a general understanding of the threats and vulnerabilities to PHI and other sensitive data staff may access or handle.
- **Incident Response.** Develop and test an incident response plan to quickly identify and mitigate potential security incidents.
- Audit Preparedness. Hospitals and their business associates should prepare for the upcoming Phase 2 audits and help minimize the risks and vulnerabilities described above by:
  - Conducting a gap assessment of current policies and procedures to confirm alignment with the Privacy and Security Rules.
  - Updating their risk analysis to identify threats and vulnerabilities to PHI and prioritize remediation items based on the criticality of and risk to the data.
  - Reviewing business associate agreements and associated policies and procedures for the oversight of service providers.
  - Developing an audit response plan or compiling a repository to have HIPAA-specific policies and procedures easily accessible and ready to provide upon request.
  - Familiarize all staff, including senior management, with the entity's privacy and security compliance program, HIPAA requirements, general risks associated with PHI, and the contact person or department for questions about these areas or any requests or inquiries from OCR or other agencies.

These takeaways are just some of the key components of a comprehensive compliance program. For additional details on applicable requirements, preventive measures or other considerations related to HIPAA compliance, please contact Tara.

Tara Cho practices in privacy and information security. As a Certified Information Privacy Professional, she advises on privacy issues and identification of potential risks and the development of associated policies and procedures to maintain compliance. She may be reached at 919.783.1079 or tcho@poynerspruill.com.

Poyner Spruill LLP

Iain Stauffer Joins Our Health Law Team

We are thrilled to announce Iain Stauffer has joined our Raleigh office. Iain came to the firm from the North Carolina Attorney General's Office, where he served as an attorney for 12 years, most recently with the Public Assistance Section. In that position, he represented the North Carolina Department of Health and Human Services and the Division of Medical Assistance in complex litigation involving Medicaid in federal and state courts. In addition, Iain provided advice and counsel in many areas of the Medicaid program, including compliance, program integrity, and managed care. Iain appeared in numerous actions at the Office of Administrative Hearings involving Medicaid audit, overpayment, reimbursement, and authorization matters.

Iain's practice at the firm will focus on advising and representing health care providers in Medicare and Medicaid reimbursement, enrollment, compliance, litigation, and regulatory issues. He may be reached at istauffer@poynerspruill.com or 919.783.2982.

Our Health Law Section

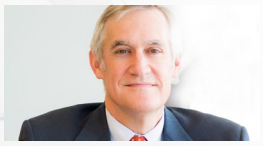
Ken Burgess
Health Law Section Team Leader
919.783.2917
kburgess@poynerspruill.com

Chris Brewer
919.783.2891
cbrewer@poynerspruill.com

David Broyles
919.783.2923
dbroyles@poynerspruill.com

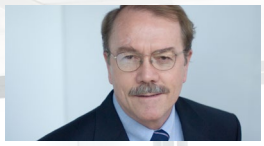
Matt Fisher
919.783.2924
mfisher@poynerspruill.com

Wilson Hayman
Corridors Editor
919.783.1140
whayman@poynerspruill.com



Todd Hemphill
919.783.2958
themphill@poynerspruill.com

Steve Shaber
919.783.2906
sshaber@poynerspruill.com



Bill Shenton
919.783.2947
wshenton@poynerspruill.com

p.s.

WWW.POYNERSPRUILL.COM