A Publication of the American Health Lawyers Association
Hospitals and Health Systems Practice Group

Volume 14 • Issue 2 • November 2012

Hospitals & Health Systems Rx

Table of Contents

Developing an Office Space Lease Compliance Program

Andrew A. Dick, Esquire*
Hall Render Killian Heath & Lyman PC
Indianapolis, IN

In today's regulatory climate, hospitals and healthcare systems are beginning to recognize that owning real estate is costly and requires sophisticated management to operate efficiently and in compliance with healthcare regulatory requirements. One of the most important issues affecting healthcare leasing arrangements is whether federal fraud and abuse laws are implicated. The federal government spends trillions of dollars on healthcare programs each year, and it estimates that fraud accounts for up to 10% of those expenditures.[1] In recent years, federal agencies have made prosecuting healthcare fraud a priority. The most commonly prosecuted federal fraud and abuse laws are the Stark Law[2] and the Anti-Kickback Statute (AKS),[3] as well as the False Claims Act.[4] These laws significantly influence leasing arrangements between hospitals and healthcare providers.

In light of the stringent requirements imposed by the Stark Law and the AKS, hospitals and healthcare providers should develop an intercompany compliance program specifically for office space leasing arrangements with potential referral sources. This article is designed to provide an overview of topics that hospitals and health systems should consider when developing such a program.

The Team

The first step in implementing a space lease compliance program is to assemble an experienced team of healthcare compliance and real estate professionals to oversee the project. The team should be led by the provider's compliance counsel and an experienced real estate attorney with healthcare compliance experience. Other team members will include the provider's real estate or facilities department, a real estate appraiser, and an architectural firm or space planner with experience measuring office space. To the extent that the provider does not manage its facilities or real estate holdings, the outside property management

firm with this responsibility should be involved in the process. An experienced team will be able to spot issues and develop best practices based on their experience. For example, an experienced real estate attorney and property manager will be able to spot arrangements that are not commercially reasonable.

When undertaking any compliance project that will involve the use of outside consultants, the provider's legal counsel should insist on each consultant executing a confidentiality agreement. The provider needs assurances that any information discovered through the compliance process is kept strictly confidential. All communications and work product should also run through legal counsel to protect the same under the attorney-client privilege and work product doctrine.

Fraud and Abuse Laws

The foundation of any space lease compliance program should be based on complying with regulations under the Stark Law and the AKS. Over the years, regulators have promulgated regulations under both that apply to space leasing arrangements. Those regulations and the guidance and commentary interpreting those regulations provide invaluable insight for any compliance program.

Space lease compliance programs should assume that all space leasing arrangements will be subject to the Stark Law and AKS. This is primarily due to the fact that the ownership within a corporate entity changes over time, and as a result, a space lease that may not initially be subject to the Stark Law or the AKS could later be subject to one or both of the laws. Therefore, this section does not include an analysis of how to determine if either law applies to the parties involved in a leasing arrangement. Instead, it assumes that all leases are subject to the Stark Law and AKS.

While many of the rules that are applicable to space leasing arrangements are similar under both laws, a high-level summary of both is worthwhile.

The AKS

Under the AKS, space leasing arrangements between regulated parties are prohibited unless the arrangement meets one of the statutes' safe harbors. A commonly used safe harbor for leasing arrangements is the *space rental safe harbor.*[5] It provides that remuneration (kickbacks, bribes, or rebates) does not include any payment made by a tenant to a landlord for the use of premises, so long as the following five conditions are met:

(1) the lease agreement is set out in writing and signed by the parties;

(2) the lease agreement specifies the premises covered by the lease;

(3) if the lease provides access to the premises for periodic intervals of time, rather than on a full-time basis, the lease must precisely specify the schedule of such intervals, including their exact length and rent for such interval;

(4) the term of the lease is for not less than one year;

(5) the aggregate rental charge is set *in advance* and is consistent with *fair market value* (FMV) in arms-length transactions; and

(6) the aggregate space rented does not exceed that which is reasonably necessary to accomplish the commercially reasonable business purpose of the rental.

While all of the conditions within the space rental safe harbor should be followed, those related to the payment of rental should be reviewed carefully. The rental rate must be "set in advance" at the time the lease is executed. This requirement means that the rental rate must be established in the agreement at the commencement of the term, without taking into account the volume or value of any referrals or business otherwise generated between the landlord and tenant.

In addition to the rent being set in advance, it must also be consistent with FMV for the space being leased. For purposes of this statute, the term "fair market value" is defined as the value of the rental property for general commercial purposes, but it should not be adjusted to reflect the additional value that one party (either the prospective landlord or tenant) would attribute to the premises *as a result of its proximity or convenience to referral sources.*[6] The FMV requirement becomes particularly important when analyzing healthcare leasing arrangements under the AKS and the Stark Law. A discussion about establishing fair market rental rates is included below in this article.

The Stark Law

The Stark Law has many similarities to the AKS, in that it targets fraud and abuse in government-run healthcare programs. To the extent that the Stark Law applies to a space leasing transaction, then an exception to the Stark Law must be found prior to entering into the leasing arrangement; otherwise, the arrangement may be in violation of the law and civil penalties may be imposed.

There are a number of Stark Law exceptions, although the *rental of office space* exception applies to most space leasing arrangements.[7] The exception allows payments for the use of office space made by a tenant to a landlord if the leasing arrangement meets the following requirements:

(1) the agreement is in writing, signed by the parties, and specifies the premises;

(2) the space to be rented does not exceed that which is reasonable and necessary for the "legitimate business purposes" of the tenant and is used exclusively by the tenant;

(3) the lease term is at least one year;

(4) the rental charge over the term of the agreement is set in advance and is consistent with FMV;

(5) the rental charge over the term of the agreement is *not* determined in a manner that: (a) takes into account the volume or value of referrals or other business generated between the parties; or (b) uses a formula based on the revenue raised, earned, billed, collected, or otherwise attributable to the services performed or business generated in the premises, or per unit of service rental charges (to the extent that such charges reflect services provided to patients referred by the lessor to the lessee); and

(6) the agreement would be *commercially reasonable* even if no referrals were made between the landlord and tenant.

The Stark Law rental of office space exception is similar to the AKS space rental safe harbor. Additionally, the Stark Law and AKS have similar FMV requirements. The Stark Law rental of office space exception provides that the leasing arrangement must be consistent with arms-length transactions, and the rental amount must be consistent with the general market value for the space. The rental amount *cannot* be adjusted to reflect the additional value that the prospective landlord and tenant would attribute to the proximity or convenience to the other where one party is a potential source of patient referrals to the tenant. The fair market rental rate cannot vary based upon volume or value of referrals.

Any space lease compliance program should be designed to ensure that all space leasing arrangements comply with both the Stark and AKS regulations discussed above.

Tax Considerations

For nonprofit, tax-exempt healthcare organizations, any space lease compliance program should also ensure that any leasing arrangement complies with various tax laws. In particular, nonprofit, tax-exempt entities entering into leasing arrangements with for-profit entities should consider four issues that may ultimately jeopardize their tax-exempt status or a benefit conferred upon the entity based upon its tax-exempt status: (1) whether the leasing arrangement would result in private inurement to the landlord or tenant; (2) whether the leasing arrangement would confer a private benefit to the landlord or tenant; (3) if the leased spaced is financed with tax-exempt bond proceeds; and (4) whether the leasing arrangement will affect a property tax exemption. A discussion of each issue is described below.

Private Inurement

Any space lease compliance plan should attempt to prevent leasing arrangements where private inurement could exist. The concept of private inurement is particularly important for nonprofit, tax-exempt entities. The concept is based on Section 501(c)(3) of the Internal Revenue Code, which states that for an entity to receive and maintain its tax-exempt status, "no part of the net earnings of [the entity] may be to the benefit of *any private shareholder or individual.*" This means that none of the income or assets of an exempt organization may be permitted to directly, or indirectly, unduly benefit a person or other entity that has a close relationship with the organization, when he, she, or it is in a position to exercise a significant degree of control over the exempt entity. The private inurement doctrine was created to ensure that tax-exempt entities further their charitable purpose and not the private interests of the directors, trustees, officers, or other interested persons—otherwise known as "insiders."[8] If a nonprofit entity is found to have violated the private inurement doctrine, its tax-exempt status could be revoked or denied.

With that in mind, any space lease compliance plan should attempt to identify proposed leasing arrangements where a tax-exempt entity is leasing space to or from a person who qualifies as an *insider,* or a for-profit entity in which an insider has an interest. The private inurement doctrine does not necessarily prevent an exempt organization from leasing space to or from an insider if the rent and other terms are reasonable and are consistent with arm's-length transactions. For example, a lease with a fair market rental rate to an insider would most likely avoid a violation of the private inurement doctrine as there would be no apparent indication of either party gaining an excess benefit from the transaction.

Private Benefit

Nonprofit, tax-exempt entities also need to incorporate safeguards into their space lease compliance plans to avoid private benefit. The private benefit doctrine requires that an exempt entity operate exclusively for exempt purposes.[9] Under this doctrine, an exempt organization will not be regarded as operating exclusively for its exempt purpose if more than an insubstantial part of its activities is not in furtherance of an exempt purpose.[10] The private benefit doctrine differs from the private inurement doctrine in that it is broader and applies to transactions with individuals or entities *that are not, or do not have members who are, insiders.* It should be noted, however, that the private benefit doctrine tolerates some incidental benefit to private parties as long as that benefit is insubstantial. Tax-exempt entities should be careful to avoid any transaction where private benefit could exist, as the Internal Revenue Service has used the doctrine to deny or revoke organizations' exempt status.[11]

When a tax-exempt organization desires to lease space to or from a for-profit entity, the private benefit doctrine will most likely apply. Therefore, the parties involved must look at whether the agreement provides more than an incidental benefit to the for-profit entity so that the transaction does not jeopardize the exempt entity's exempt status. An exempt organization is designed to operate for charitable purposes, and as a result, the majority of its activities/benefits should be dedicated to its charitable purpose, and the private benefit the lease confers should be insignificant in comparison. The exempt organization should also look at the lease terms to make sure that it is agreeing to what could be considered necessary to effect its exempt purpose and that the terms and the price do not provide any unnecessary benefit to the for-profit party. For example, where a hospital leases space to a for-profit entity for necessary services at FMV, and for as long as those services are needed for the hospital to effect its charitable purposes, the arrangement should not violate the private benefit doctrine.

Private Business Use

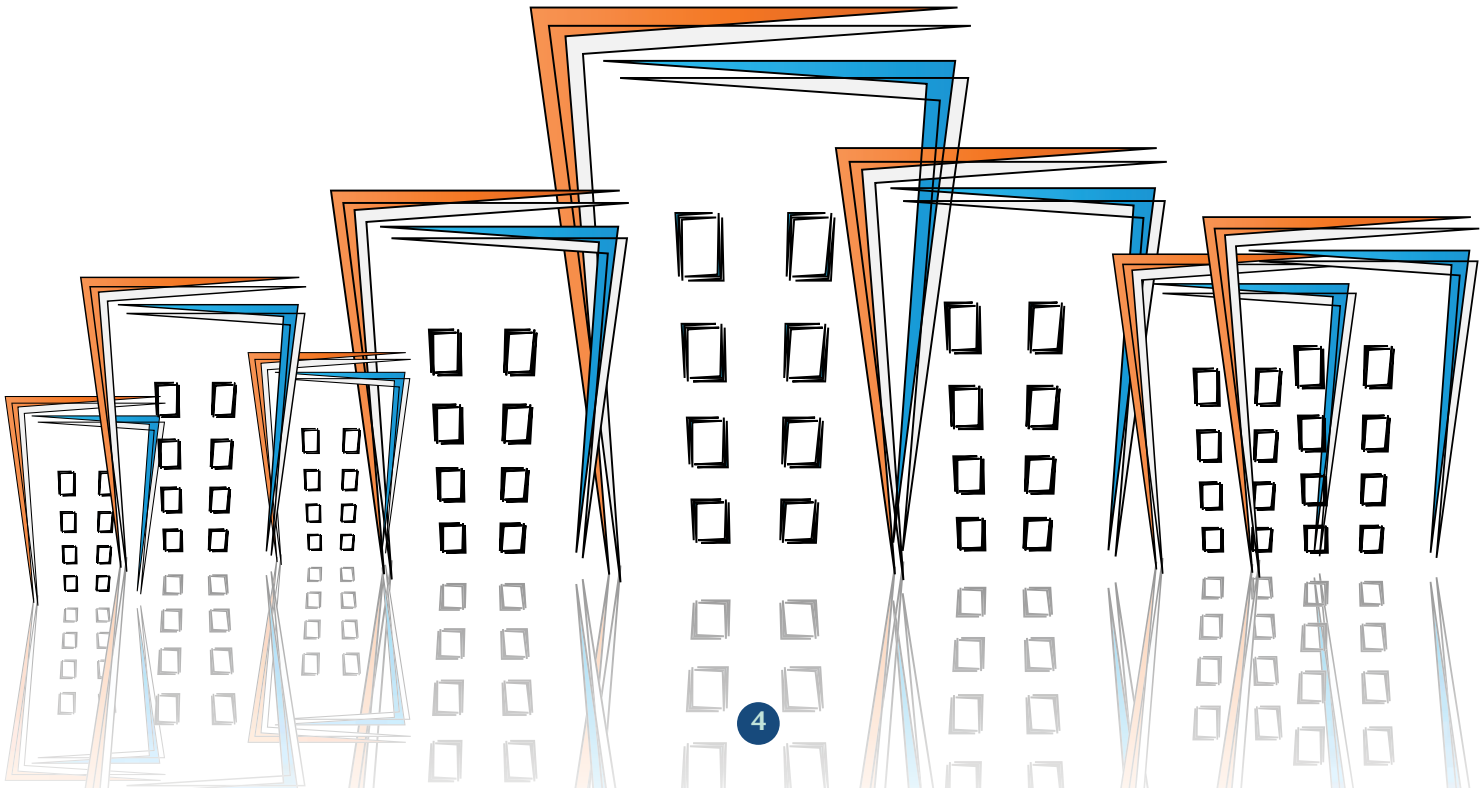
When a tax-exempt organization finances the construction or purchase of a facility using tax-exempt bonds, the facility is subject to certain use restrictions. This is primarily the case because the purchaser of the bonds and the borrower receive certain tax benefits based on the tax-exempt status of the borrower entity. As a condition of receiving preferential tax treatment, the facility financed cannot be used for any "private business use."[12]

Section 1.141-3(b)(3) of the Treasury Regulations provide that the lease of bond-financed property to a private actor (i.e., a non-governmental person for purposes of governmental bonds or use other than by a qualified 501(c)(3) organization engaged in an activity related to its exempt purpose, in the case of Qualified 501(c)(3) bonds) is private business use of the property. For this purpose, any arrangement that is properly characterized as a lease for federal income tax purposes is treated as a lease. Failure to comply with these federal tax requirements can jeopardize the preferential tax status of the bonds. It should be noted that, in some cases, short-term leasing arrangements to a for-profit user are permitted, although that is the exception rather than the rule.[13]

To the extent that the provider has financed a facility with tax-exempt bonds, the space lease compliance plan should include additional guidelines to address private use concerns.

Property Tax Exemptions

Finally, any space lease compliance program should attempt to identify any property tax exemptions that apply to the space



owned or leased by a provider. In many cases, property tax exemptions have specific ownership and use requirements. If the space is leased to an individual or for-profit entity that fails the ownership or use requirement, the exemption could be denied or revoked. The compliance team that is developing the compliance program should incorporate any property tax exemption requirements into the program.

Inventory Real Estate Holdings

After the team understands the scope and purpose of the compliance plan, it is essential to prepare an inventory of the provider's real estate holdings. The inventory should identify properties that are owned and those that are leased by the provider. For leased properties, the compliance team should audit all existing lease agreements. The scope of the audit should identify the core lease terms, the amount of space leased, the owner of the building, and the make-up of the building owner (e.g., whether or not physicians or healthcare providers hold an ownership interest). The result of the audit should be a summary report or abstract of the lease agreements. That abstract can then be used to identify noncompliant lease arrangements that need to be addressed going forward.

After preparing the audit, the compliance team should identify use restrictions imposed on any buildings regardless of whether or not the buildings are owned or leased by the provider. In some cases, a title search may be necessary to identify restrictive covenants in the chain of title if the provider does not have complete records of the property history. Additionally, the compliance team should determine if any owned properties are subject to tax-exempt bond financing arrangements or any property tax exemptions. As noted above, bond-financed space is generally subject to prohibitions against use by private or for-profit entities. Along the same lines, a property tax exemption is often conditioned upon the space being used for an exempt purpose.

Space Measurements

Once the compliance team has taken an inventory of its real estate holdings, it should undertake a space measurement audit for any property for which the provider is the landlord or tenant. The space measurement audit allows the provider to adequately describe the leased space. Knowing the amount of space leased is important because it is a factor when determining if the amount of rent to be paid under the leasing arrangement is FMV. This is particularly true because fair market rental valuations establish rental rates on a per-square foot basis. It is also important from a business perspective to ensure that the provider is not overpaying in cases when it is the tenant or losing revenue when it is the landlord.

The legal counsel for the compliance team should engage an architect or space planner to assist with measuring all of the provider's real estate holdings. Because measurement methodologies vary, the compliance team should work with the architect or space planner to agree upon a measurement methodology going forward. For purposes of measuring office space, most providers elect to use a measurement standard approved by the Building Owners and Managers Association (BOMA). Providers often prefer BOMA standards because they are often employed by institutional real estate owners and investors, which supports the case that the provider's approach is commercially reasonable.

FMV Opinions

The FMV requirement becomes particularly important when analyzing healthcare leasing arrangements under the Stark Law and AKS. It is also important for nonprofit, tax-exempt organizations to ensure that their rental rates are consistent with FMV when leasing to a for-profit entity as noted above. In most cases, the provider and its staff are not qualified or sufficiently objective to establish fair market rental rates. Therefore, providers are encouraged to engage an experienced real estate appraiser or commercial real estate broker to provide a written opinion of value. While appraisals or opinions of value are not required under the Stark Law or the AKS, an independent valuation will provide evidence that the provider took substantial steps to ensure that it was entering into FMV leasing arrangements.

The selection and engagement of a real estate appraiser or commercial real estate broker should be carefully documented. While commercial real estate brokers often provide valuable opinions, an experienced real estate appraiser is the gold standard. The real estate appraiser should have the Member of the Appraisal Institute designation from the Appraisal Institute together with experience valuing medical office or hospital space, as the case may be, in the community where the subject property is located. If a commercial real estate broker is selected for the project, he or she should have significant experience valuing office space in the community where the subject property is located.

The compliance team should establish criteria for engaging a valuator to provide an opinion of market rental rates. The criteria should include a mandate that in-house or outside counsel always engages the valuator for the benefit of the provider. Engaging the valuator through counsel is designed to protect the communications between legal counsel and the valuator under the attorney-client privilege and any reports issued under the work-product doctrine.

This author prefers to engage valuators through an engagement letter that outlines the scope of work to be performed by the valuator. The engagement letter should include the following:

- The location and type of property to be valued;
- Type of rent rate methodology to be used (e.g., gross versus net);
- Type of building services offered to the tenant;
- The length of the proposed lease terms;
- Tenant improvement allowances offered;
- Definitions of FMV under the Stark Law and the AKS should be used for valuation purposes;

- All communications about the project and the report should be issued to legal counsel;
- The rental rate should be issued in the form of a range of FMV; and
- The report should be issued in draft form.

The opinion of market value should be issued in the form of a range to offer the provider with some flexibility when negotiating rental rates. The valuator should also indicate how the provider should select a rental rate within the range. For example, space with higher-quality finishes may command a higher rental rate. The engagement letter may also specify whether rental rate escalators or tenant improvement allowances are generally offered to tenants in the market.

The provider should always keep in mind that valuators may be called to testify and defend their opinions of value. A qualified and experienced valuator will likely serve as a better witness in a case where fair market rates are challenged.

Approval Process; Disclosure Reporting

The compliance plan should outline the process of negotiating and approving a new space lease. In order to ensure that the technical requirements imposed on leasing arrangements are satisfied, multiple layers of approval are encouraged. While the property management team should assume the responsibility for administering lease agreements, the finance or accounting departments and possibly the chief executive should be involved in approving any new space lease agreements. Involving several departments and requiring each to physically sign off on the proposed arrangement helps to ensure that the compliance requirements are met. It also forces high-level employees to assume ownership for the arrangements.

The property management team and the responsible administrators who will sign off on the arrangement should document the approvals using a contract approval form. The contract approval form should describe the responsible property management employee who is in charge of the arrangement and the administrators that will ultimately approve the arrangement. The contract approval form should force the responsible property management official to confirm the following:

- The terms of the space lease comply with the Stark Law and AKS office space lease exceptions;
- The space being leased has been measured and the square footage is accurately set forth in the space lease;
- The rental rate entered into the space lease is within the range of fair market rates for the space as documented by the provider through valuations;
- The permitted use in the space lease will not jeopardize any property tax exemption and/or tax-exempt bonds allocated to the space; and
- The contracting parties are not excluded from participating in Federal Procurement and Nonprocurement Programs or by the U.S. Department of Health and Human Services Office of Inspector General (OIG).

In addition to developing a hierarchy of approvals before a space lease is executed, the compliance team should also develop a disclosure protocol for potential space lease arrangements that may violate any of the fraud and abuse laws or tax laws contemplated herein. A space lease compliance plan should incorporate a process whereby noncompliant arrangements are identified and reported to compliance counsel and a brief report issued to high-level administrators.

Education

Any compliance plan should incorporate an educational component where members of the compliance team educate staff members involved in property management. The compliance team should educate members of the property management team on fundamental real estate concepts, focusing on different rental rate methodologies, how space is measured, negotiating rental rates, and tenant improvement allowances.

The compliance team should incorporate regulatory guidance and case law as a means of describing noncompliant leasing arrangements. A good starting point is a Special Fraud Alert[14] that OIG issued, describing "questionable" leasing arrangements that the AKS is designed to prohibit:

- Rental amounts in excess of amounts paid for comparable property rented in arms-length transactions between persons not in a position to refer business;
- Rental amounts for subleases that exceed the rental amounts per square foot in the primary lease;
- Rental amounts that are subject to modification more often than annually;
- Rental amounts that vary with the number of patients or referrals;
- Rental arrangements that set a fixed rental fee per hour, but do not fix the number of hours or the schedule of usage in advance (i.e., "as-needed" arrangements);
- Rental amounts that are only paid if there are a certain number of federal healthcare program beneficiaries referred each month; and
- Rental amounts that are conditioned upon the supplier's receipt of payments from a federal healthcare program.

Another practical example comes from *United States ex rel. Goodstein v. McLaren Regional Medical Center,* 202 F. Supp. 2d 671 (E. D. Mich. 2002), where a qui tam action revealed the challenges in determining fair market rental rates.

Annual Compliance Audits

Finally, any compliance plan should incorporate an annual review of existing space lease agreements and leasing practices. The goal is to identify arrangements that may not have been documented

properly or that may be out of compliance due to a change in circumstances. Members of the property management team should also walk existing buildings on a periodic basis to determine how space is being occupied and by whom.

Conclusion

Developing a space lease compliance plan can be complex. This article is designed to serve as a framework for a provider intending to develop a space lease compliance plan, although it is not designed, nor intended, to be comprehensive. Providers are encouraged to enlist the services of experienced healthcare compliance attorneys and real estate attorneys with compliance experience when developing a compliance plan. The more experienced the team, the better the chances are that the provider will avoid costly compliance issues going forward.

**Andrew Dick is an attorney in the Indianapolis office of Hall Render Killian Heath & Lyman PC and the current Chair of AHLA's Real Estate Affinity Group. He can be reached at (317) 977-1491 or at adick@hallrender.com.*

Portions of this article under the headings of Private Benefit and Private Use were previously published by the American Bar Association (ABA) in connection with a speech given by the author titled "Medical Office Leases: Understanding the Regulatory Requirements Behind the Lease Terms" at the ABA Real Property, Trust & Estate Spring Symposia in 2009.

1 Foster, R.S., et al. Updated and Extended National Health Expenditure Projections, 2010-2019, Centers for Medicare & Medicaid Services, June 29, 2009, *available at* www.cms.gov/NationalHealthExpendData/downloads/NHE_Extended_Projections.pdf (last visited September 25, 2012).

2 42 U.S.C.S. § 1395nn.

3 42 U.S.C. § 1320a-7b.

4 31 U.S.C.S. § 3729-3733.

5 42 C.F.R. § 1001.952(b).

6 42 C.F.R. § 1001.952(b)(6) (emphasis added).

7 42 U.S.C. § 1395nn(e)(1)(A).

8 An "insider" is generally considered one who has a unique relationship with the exempt organization where the individual (or corporation) "can cause application of the organization's funds or assets for the private purposes of the person by reason of the" person's position to exercise and control over the organization. Bruce R. Hopkins, The Law of Tax Exempt Organizations, 510 (10th ed. 2011) (citing *American Campaign Academy v. Comm'r,* 92 T.C. 1053 (1989). Insiders may include an organization's founders, trustees, directors, officers, key employees, members of the family of these individuals, and certain entities controlled by them. *Id.*

9 Treas.Reg. §1-501(c)(3)-1(c).

10 *Id.*

11 Bruce R. Hopkins, Nonprofit Law Insights: Beware the Private Benefit Doctrine, *available at* http://newsletterlink.pkfnan.org/pkfnan/article.asp?cid=32&nid=9&pid=341s0145be251e452w4eut2l&aid=375&issue=Fall+2001 (last visited September 25, 2012).

12 26 U.S.C.A § 145(a)(2); 26 U.S.C.A § 141.

13 Treas. Reg. § 1.141-3(d)(3)(i) and (ii).

14 Special Fraud Alert, February 2000 - Rental of Office Space in Physician Offices by Persons or Entities to which Physicians Refer, *available at* https://oig.hhs.gov/fraud/docs/alertsandbulletins/office%20space.htm (last visited October 1, 2012).

It's 2 AM: Do You Know Where Your Patients' Information Is?

D. Brent Wills, Esquire
Gilpin Givhan PC
Montgomery, AL

On September 17, 2012, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced that it had entered into a resolution agreement (i.e., settlement) with Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates (collectively, MEEI) which required MEEI to pay $1.5 million to OCR and enter into a three-year corrective action plan with the agency. The agreement related to the theft of a laptop belonging to an MEEI-affiliated physician while the physician was lecturing in South Korea in 2010. Although the laptop included certain data security features, it was not encrypted. The laptop reportedly held protected health information (PHI) for more than 3,600 of MEEI's patients.

Unfortunately, the MEEI breach involves facts that are becoming all too familiar as hospitals and other "covered entities" struggle to maintain the privacy and security of their patients' personal information, as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1] For example, the following are among the largest hospital breaches so far in 2012:

- Emory University Hospital in Atlanta, GA, misplaced ten unencrypted backup computer disks containing PHI for more than 300,000 individuals. The disks contained old data from software the hospital deactivated years ago. Although the disks were stored in an office that was locked at night, they went missing from an unlocked storage cabinet.
- At Howard University Hospital in Washington, DC, an employee of a business associate of the hospital downloaded patients' PHI to a personal laptop computer, in violation of the hospital's data security policies. The laptop was subsequently stolen from the employee's vehicle. Even though the laptop was password protected, it was not encrypted. The laptop contained PHI for more than 34,000 individuals.
- Memorial Healthcare System in Hollywood, FL, discovered that two employees had stolen PHI for nearly 10,000 patients with the intent to use it to file fraudulent tax returns.

Like MEEI, all three hospitals reported the incidents to OCR pursuant to requirements in the Health Information Technology for Economic and Clinical Health Act (HITECH), part of the 2009 federal stimulus legislation.[2] All three now appear on OCR's website listing of "major" breaches that affect 500 or more individuals (the so-called Wall of Shame). Undoubtedly, all three hospitals have already suffered considerable economic and noneconomic losses in dealing with their respective breaches. Moreover, OCR presumably will investigate each of the breaches, and, if the MEEI breach is an indicator, one or more of the hospitals may be subject to significant civil monetary penalties (CMPs) to boot.

Why Should Hospitals be Worried?

Data breaches are occurring at an alarming rate in all industries, but particularly in the financial sector and in healthcare. OCR data indicates that since September 2009, when the HITECH breach notification requirement became effective, the agency has received nearly 60,000 notifications[3]—that is, 60,000 breaches reported in roughly 1,000 days. Frighteningly, the number of breaches reported during 2011 increased nearly one-third from 2010.[4] In addition, the author recently learned from an OCR spokesperson that, during 2012, a particular regional office of OCR is receiving an average of four major breach notifications per month.

The potential costs and legal risks associated with data breaches are substantial. Any breach that occurred on or after February 18, 2009, is subject to the CMP scheme established by HITECH.[5] Whereas maximum CMPs for HIPAA violations were previously capped at $25,000, HITECH authorized penalties up to $1.5 million per violation.[6] Not surprisingly, OCR has been quick to flex its HITECH enforcement muscle to negotiate a number of resolution agreements that have often entailed substantial resolution payments; for example, in addition to the $1.5 million payment from MEEI, OCR has received resolution payments this year in the amounts of $1.7 million and $1.5 million, respectively, from the Alaska Department of Health and Social Services (Alaska DHSS) and Blue Cross Blue Shield of Tennessee (BCBSTN). Significantly, these three resolution agreements represent the first publicized enforcement actions taken by OCR against covered entities that reported data breaches pursuant to HITECH's requirements (i.e., self-reported potential HIPAA violations). HITECH also authorizes state attorneys general (AGs) to pursue CMPs with respect to data breaches and other HIPAA violations that affect their constituents.[7] Several AGs have seized upon this power, including Massachusetts

AG Martha Coakley, who earlier this year entered into a $750,000 settlement with a Boston hospital to resolve federal HIPAA and state law claims relating to a 2010 data breach. It is noteworthy that there was no showing, in any of these cases, that PHI was inappropriately accessed or misused.

Even if no penalties or settlement payments result, however, data breaches may still be very costly. For example, in the wake of a breach, a hospital may need to engage legal counsel, information technology consultants to assist with internal investigations and corrective actions, and a public relations firm to help notify the individuals affected by the breach (and, in some cases, the media) and to help with damage control for the hospital's public image. The hospital may also incur significant costs to correct any security problems that contributed to the breach (e.g., updating or upgrading technology, policies and procedures, or physical safeguards). Consider, also, that OCR investigates every major breach notification it receives. The cost of dealing with an investigation—again, even where no penalties result—may be substantial. As an example, reports indicate that, whereas BCBSTN ultimately paid $1.5 million to OCR pursuant to its resolution agreement, it spent nearly $17 million to conduct an internal investigation, implement corrective actions, notify the affected individuals, and deal with OCR.[8] Ironically, BCBSTN may have gotten off light: studies have determined that data breaches—especially those that entail media notifications and government investigations—may cost hospitals as much as $500 per affected individual.[9] None of this accounts, of course, for lost time and productivity, or for other, indirect economic harm a breach may cause to a hospital's brand and reputation.

What's more, while cyber espionage gets headlines, OCR statistics show that a substantial majority of breaches result from simple breakdowns in everyday privacy and security practices. Specifically, breaches most frequently result from theft or loss, inadequate safeguards, or improper disposal of PHI, and they most frequently involve PHI in paper format or electronic PHI stored on unencrypted portable electronic devices, such as laptop computers, flash drives, and smart phones. The MEEI, Alaska DHSS, and BCBSTN breaches, for example, all resulted from theft of unencrypted portable devices. Indeed, in its enforcement actions against MEEI and Alaska DHSS, OCR put portable devices front and center, identifying various alleged deficiencies and calling for a number of corrective actions specifically targeting such devices.[10] By comparison, only a very small percentage of breaches reported to OCR have involved computer hackers. This is not to say, of course, that hackers are not a threat to a hospital's e-PHI; on the contrary, they are a major threat. What it does say is that the data breach problem is far more than just "an IT issue."

Other studies have determined that more than 80% of physicians (and presumably most clinical and administrative staff, as well) use smart phones or other portable electronic devices in their work. This, in and of itself, should not be surprising. But consider that the majority of those devices are not encrypted or lack necessary data security safeguards. As the MEEI, Alaska DHSS, and countless other breaches exemplify, any physician or medical staff member, any management personnel, or any other hospital workforce member walking around with an unencrypted laptop, smart phone, or jump drive that contains patients' PHI may be a breach waiting to happen. Worse, other studies have suggested that the street value of a medical identity may be up to fifty times greater than the value of a Social Security number. Criminals are wise to this. A significant market has developed for stolen PHI; as illustrated earlier, a common tactic is to use stolen patient information to file fraudulent tax returns.

Perhaps it is not surprising, then, that, more often than not, data breaches are caused by insiders. This means that someone in a hospital's workforce, or in the workforce of the hospital's business associate, either does not have a proper understanding of his or her responsibilities in regard to PHI or, more and more frequently, has intentionally violated those responsibilities. Again, the illustrations at the beginning of the article reflect classic cases: in one case, a contractor failed to follow the hospital's policy; in the other, a hospital employee simply stole patients' PHI.

In sum, data breaches are happening to everyone, everywhere. Not even the healthcare elite are excluded. MEEI, for example, is the primary ophthalmology and otolaryngology teaching hospital for Harvard Medical School, and it has experienced large breaches both before and since the breach that led to its resolution agreement with OCR. Likewise, in addition to the Emory University Hospital breach referenced above, Stanford University Hospital has experienced multiple large breaches during the last two years, including a breach last year that impacted nearly 20,000 emergency room patients. Similarly, both the UCLA Health System and the M.D. Anderson Cancer Center have reported or experienced multiple large breaches, the latter on three separate occasions in 2012 alone. All these breaches involved either theft or loss of an unencrypted portable electronic device or inappropriate access, use, or disclosure of PHI by a member of the hospital's workforce or a business associate.

What Comes Next?

With the advent of telemedicine, cloud computing, and mobile health, among other advances, the healthcare industry is constantly turning out new and improved technologies. New technologies, however, mean new challenges for hospitals and other covered entities in regard to information privacy and security. From OCR's perspective, each new challenge presents a new opportunity for enforcement.

In addition, OCR, pursuant to a Congressional mandate in HITECH, recently commenced its first-ever HIPAA compliance audits. OCR entered an agreement last year with KPMG to develop an audit protocol and conduct an initial "pilot" round of 115 compliance audits expected to be completed by the end of 2012.[11] OCR recently published the HIPAA audit protocol, but it has not published any specific audit results. Further, the future of the audit program remains unclear; OCR's contract with KPMG only covers the initial round of audits. OCR has indicated informally that compliance audits will continue beyond 2012, but it has not addressed, for example, whether, when, or to what extent there will be an expanded rollout of the program. Whatever the

future of the HIPAA audits, however, the program is only one piece in a larger enforcement trend.

It is also expected that OCR will soon publish its long-awaited "omnibus" final HITECH regulation (HITECH Final Rule) that will finalize and implement many of the Act's provisions. Among other things, the HITECH Final Rule will finalize and implement important changes to the HIPAA privacy rule, including expansions to individuals' rights to access their own PHI, new restrictions on certain uses and disclosures of PHI that involve financial remuneration, new requirements relating to the use of PHI in connection with fundraising, and important changes to business associate agreements and notices of privacy practices. All these new compliance obligations, again, represent new enforcement opportunities for OCR. Hospitals and other covered entities must be in compliance with most of the requirements of the HITECH Final Rule within 240 days after the rule is published.[12]

Finally, class action lawsuits are gathering steam. Stanford Hospital and its business associate, Multi-Specialty Collection Services, for example, are facing a $20 million class action suit in regard to the 2011 data breach mentioned above. Likewise, Emory Hospital is facing a $200 million class action suit involving more than 200,000 plaintiffs in regard to its breach reported earlier this year. Moreover, although HIPAA does not provide for individual causes of action, HITECH directed OCR to develop procedures whereby individuals who notify OCR about violations (i.e., whistleblowers) may receive a percentage of any penalties or other amounts the government ultimately recovers.[13] OCR missed its February 2012 target date to promulgate regulations to implement the whistleblower mandate, but there is nothing to indicate that OCR will not move forward with this initiative.

What Should Hospitals Do?

The discussion above indicates, loud and clear, that the government has taken on a distinctly enforcement-oriented mindset in regard to HIPAA. Given the very high likelihood that most or all hospitals will experience a data breach, combined with the potential for future compliance audits, and potentially even whistleblower and class action lawsuits, it behooves hospital management to take on an enforcement-oriented mindset as well—i.e., "Not if, but when."

In preparing to deal with OCR, a hospital's primary objective should be to demonstrate that violations, if any, resulted from reasonable cause, and not willful neglect. Under the HITECH penalty scheme, this could be the difference between a $1,000 per-violation penalty, or no penalty at all,[14] and a *minimum* $50,000 per-violation penalty, up to an aggregate maximum of $1.5 million per violation. In this regard, OCR guidance indicates that putting policies and procedures and other basic safeguards in place and demonstrating a good-faith effort to comply are indicators of reasonable cause, whereas failure to put such safeguards in place is an indicator of willful neglect.[15] This is consistent with OCR's resolution agreements to date; these have focused heavily on covered entities' failure to implement very basic protections, particularly security risk analysis, compliance programs and policies and procedures, workforce training and accountability practices, physical safeguards, and audit and monitoring mechanisms. Also, as mentioned above, recent enforcement activity suggests that OCR is zeroing in on information safeguards on portable electronic devices.

Moreover, at least in general, OCR appears to be interested as much in a covered entity's overall HIPAA compliance process as it is in particular breaches and deficiencies. Hospital management must take the initiative to conduct a security risk analysis to identify the particular security risks and vulnerabilities associated with its patients' PHI and develop reasonable and appropriate safeguards to address those risks and vulnerabilities. The hospital must also regularly update its security risk analysis and evaluate whether its existing safeguards are effectively protecting its patients' PHI; if not, the hospital must promptly take corrective action. In addition, each step in the process must be consistent with the others. A top notch compliance program and set of policies and procedures is not worth much—from OCR's perspective—to a hospital that does not train its workforce or hold them accountable for noncompliance. The process must also be constantly adapting to reflect changes in the hospital's workforce and operations, changes in laws and technology, and security risks and vulnerabilities identified by the hospital. Finally and perhaps most importantly, hospital management must thoroughly document the steps the hospital takes to follow its compliance program and policies and procedures. In an enforcement battle with OCR, thorough documentation of compliance may be a hospital's most valuable weapon.

In addition, as part of a hospital's HIPAA compliance process, management must thoroughly vet the hospital's information technology vendors and other business associates. Management should closely examine a prospective vendor's privacy and security practices, for example, and confirm that the vendor does not appear on the Wall of Shame. Management should also ensure that the hospital's vendor and business associate agreements include rights to indemnification and other protections sufficient to compensate the hospital in the event of a data breach or other information security incident.

A hospital's compliance process must also address encryption. While technically not required by HIPAA, OCR has clearly indicated a strong preference for encrypting e-PHI on multiple fronts. In its resolution agreement with MEEI, for example, OCR

emphasized MEEI's failure to address whether, in its particular circumstances, encryption was a reasonable and appropriate e-PHI safeguard. In addition, OCR exempts e-PHI encrypted pursuant to standards established under HITECH from the Act's breach notification requirements.

Finally, hospitals should be aware that HIPAA and HITECH provide an affirmative defense against CMPs for covered entities that correct potential violations within thirty days, absent evidence of willful neglect.[16] Thus, a hospital's HIPAA compliance program and policies and procedures, and its overall HIPAA compliance process, should require the hospital to take steps to correct any breach of PHI or other potential HIPAA violation within thirty days, or as soon as reasonably practicable.

1 42 USC § 1320d-5 and -6; *see also* 45 CFR Part 160 and Part 164, Subparts, A, C, D, and E.

2 *See* Division A, Title XIII and Division B, Title IV, American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, at § 13402 (HITECH).

3 *See* David Holtzman, OCR, Breach Notification for HIPAA Covered Entities and Business Associates, *available at* http:/csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-4_dholtzman_ocr-hitech-breach-notifcation-rule.pdf.

4 *See* Brian T. Horowitz, *Health Care Data Breaches Increase by 32 Percent: Ponemon Report*, Health Care IT News (December 1, 2011), *available at* www.forbes.com/sites/andygreenberg/2010/11/08/data-spills-cost-u-s-hospitals-6-billion-a-year/?boxes=Homepagechannels.

5 *See* HITECH, at § 13410(d)(2), *codified at* 42 USC § 1320d-5(a)(3).

6 *See Id.*

7 *See* HITECH, at § 13410(e)(1), *codified at* 42 USC § 1320d-5(e).

8 Press Release, Blue Cross, HHS Reach Settlement in 2009 Hard Drive Data Theft (Mar. 13, 2012), *available at* www.bcbst.com/about/news/releases/default.asp?release=426.

9 *See* Andy Greenberg, *Data Spills Cost U.S. Hospitals $6 Billion A Year*, Forbes (Nov. 8, 2010), *available at* www.forbes.com/sites/andygreenberg/2010/11/08/data-spills-cost-u-s-hospitals-6-billion-a-year/?boxes=Homepagechannels (reporting on 2010 study published by Ponemon Institute).

10 *See* Resolution Agreement by and between OCR and MEEI dated September 13, 2012, at 1-2, *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement-pdf.pdf and Resolution Agreement by and between OCR and Alaska DHSS dated June 25, 2012, at 6, *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.pdf.

11 *See* Audit Pilot Program, *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html.

12 *See* HITECH, at § 13405.

13 *See* HITECH, at § 13410(b)(2).

14 OCR retains discretion to waive penalties due to reasonable cause and not willful neglect. *See* 42 CFR § 160.412; *see also* Enforcement IFR, 74 Fed. Reg. at 56129. Penalties are mandatory, however, for violations that involve willful neglect. *See* 42 CFR § 160.404(b)(2)(iv).

15 *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed. Reg. 40868, 40879 (July 14, 2010).

16 *See* 45 CFR § 160.410(a)(3).

Hospitals and Health Systems Practice Group Leadership

Hal McCard
Chair
Community Health Systems
Franklin, TN
(615) 628-6520
hal_mccard@chs.net

Andrew J. Murray, Vice Chair – Publications
Bradley Arant Boult Cummings LLP
Nashville, TN
(615) 252-2366
amurray@babc.com

Thomas M. Donohoe
Social Media Coordinator
Polsinelli Shughart PC
Denver, CO
(303) 583-8257
tdonohoe@polsinelli.com

Lisa M. Ohrin, Vice Chair – Research and Website
Health Management Associates (HMA)
Naples, FL
(239) 552-3668
lisa.ohrin@hma.com

Mary Beth Fortugno, Vice Chair – Educational Programs
Bass Berry & Sims PLC
Nashville, TN
(615) 742-7739
mfortugno@bassberry.com

Claire M. Turcotte, Vice Chair – Strategic Activities
Bricker & Eckler LLP
West Chester, OH
(513) 870-6573
cturcotte@bricker.com

Albert 'Chip' D. Hutzler, Vice Chair – Membership
HealthCare Appraisers Inc.
Delray Beach, FL
(561) 330-3488
chutzler@hcfmv.com

What is Keeping You Up at Night? In-House Counsel Try to Keep Up Without Staying Up

Michelle Bergholz Frazier, Esquire
Frazier Law Office
Milwaukee, WI

In contrast to the days when transactional work made up most of an in-house counsel's daily tasks, today's counsel is preoccupied with keeping ahead of increasingly aggressive compliance initiatives, while still getting the rest of the work done. As we all know, the healthcare climate has changed significantly, and the HEAT[1] is on for in-house legal counsel. In fiscal year (FY) 2010, the U.S. Department of Health and Human Services (HHS) and U.S. Department of Justice recovered a record-breaking $4 billion through fraud prevention and enforcement efforts, along with more than $2.5 billion from civil healthcare matters brought under the False Claims Act (FCA).[2] From 2010 to 2011, criminal healthcare fraud prosecutions increased by 68.9%,[3] and the federal FY 2013 budget will increase funding for fraud enforcement activities by 92% more than the FY 2011 budget.[4]

These changes go hand in hand with the Affordable Care Act's[5] (ACA's) reported successes in combating healthcare fraud through additional anti-fraud measures, such as enhanced screenings and enrollment requirements, increased data sharing across government, and expanded overpayment recovery efforts. The federal government converted its historical pay-and-chase approach to fighting healthcare fraud and is seeing results. But these changes also include new requirements that affect an in-house counsel's job on a daily basis. The following are just a few of the issues that stem from these new initiatives.

Sixty-Day Window for Return of Overpayments

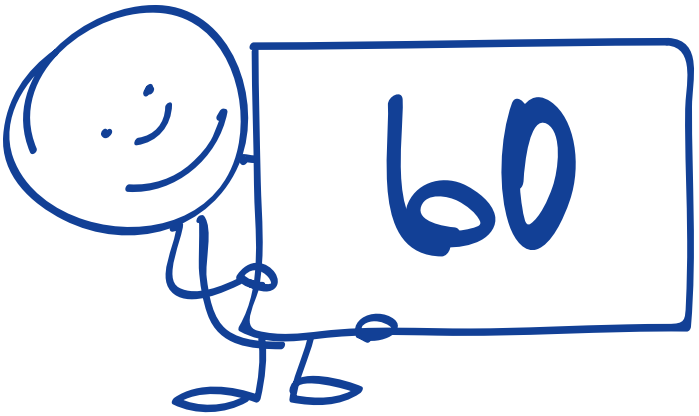
In 2009, the Fraud Enforcement and Recovery Act (FERA) expanded FCA liability to the retention of overpayments where there is a knowing and improper concealment or avoidance of an obligation.[6] As amended by FERA, liability under the FCA was expanded to specifically include improper retention of an overpayment of federal funds. Improper retention of overpayments may now trigger treble damages and penalties of $5,500 to $11,000 per claim under the FCA. The FERA amendments did not specify, however, the point at which improper retention of an overpayment would trigger FCA liability, leaving counsel scratching their heads about when due diligence stretches beyond acceptable timeframes.

Section 6402(a) of the ACA somewhat answered this question by codifying FERA's duty to repay and creating an obligation to repay by the later of sixty days after the overpayment is identified (meaning likely after due diligence has been performed) or the date the corresponding cost report is due.[7] The ACA further states that "[a]ny overpayment retained by a person after the deadline for reporting and returning the overpayment . . . is an obligation [as defined in the False Claims Act]."[8]

Although this additional guidance is helpful, in-house counsel still are left worrying about triggering false claims liability with every compliance investigation. When is an overpayment officially "identified?" Are we allowed to conduct due diligence regarding potential overpayments before triggering a repayment timeline? In February, the Centers for Medicare & Medicaid Services (CMS) published in the *Federal Register* its much-anticipated notice of proposed rulemaking regarding Medicare obligations to report and return overpayments (Proposed Rule).[9] In its Proposed Rule, CMS interprets the identification of an overpayment to be the time at which a person acts with actual knowledge of, in deliberate ignorance of, or with reckless disregard to, the overpayment's existence.[10] If the reasonable inquiry reveals an overpayment, the provider then has sixty days to report and return the overpayment.[11] Failure to make a reasonable inquiry also could result in a provider being deemed to have knowingly retained an overpayment.[12]

This new guidance adds clarification to the sixty-day rule for in-house counsel, but complex billing errors and more complicated compliance issues may be difficult to sort out within sixty days. In such cases, patient records need to be reviewed, billing practices need to be investigated, and complex reports must be run. The Proposed Rule fails to provide guidance on how counsel should handle complex issues when it is impossible to quantify overpayments within a two-month timeframe.

As a result, in-house counsel are left with uncertainty and are forced to creatively build sixty-day timeframes into their response strategies. The goal is to establish proof against allegations that the organization recklessly or deliberately ignored evidence of an



overpayment. For example, counsel should encourage personnel involved in investigations to keep daily logs showing when evidence was received, when the investigation started, and when steps were taken. These investigations should then be reviewed regularly to monitor progress and determine if the organization has officially identified an overpayment. Response strategies ultimately should be tailored to this new timeline and uncover the following information:

- How the error was discovered;
- The reason for the overpayment;
- A description of the provider's corrective action plan to ensure that the error does not reoccur;
- The timeframe during which the situation that led to the error existed, and the total amount of the refund the provider has calculated for claims submitted during that timeframe; and
- Where applicable, a description of any statistical sampling and statistical methodology used to determine the amount of the overpayment.[13]

Ten-Year Look-Back Period

In the same Proposed Rule described above, CMS also set forth a new look-back period for compliance reviews. The Proposed Rule specifically requires overpayments to be reported and returned if a person identifies the payment within ten years of the date the overpayment was received. This new look-back period is four to six years longer than look-back periods typically applied by in-house counsel.[14] Indeed, the FCA statute of limitations generally requires the government to bring its action within six years of a violation, or within three years of the date that the government learns, or should have learned, that a violation occurred or might have occurred, whichever is last.[15] Medicare Conditions of Participation require providers to maintain medical records for only five years,[16] and a limitation period of six years applies for civil monetary penalties.[17] For hospitals and other providers submitting cost reports, the reopening rules state that Medicare contractors may reopen claims within one year for any reason, within four years for "good cause," and any time if evidence of fraud or similar fault exists.[18]

Nevertheless, CMS reportedly included a ten-year look-back period in its Proposed Rule to furnish counsel with reasonable certainty after a certain period of time that they can close their books and not have ongoing liability associated with an overpayment. But as noted above, a ten-year look-back period cuts against established practices, including accepted record retention policies that typically permit destruction prior to ten years. As such, necessary documentation may not be available if required to implement the Proposed Rule's ten-year look-back period. This, coupled with the fact that memories fade and employees leave, makes a ten-year look-back period enough to keep any in-house counsel awake at night.

Technical Stark Violations

The federal physician self-referral statute (Stark) prohibits most financial arrangements between healthcare providers and referring physicians, unless the arrangements meet all elements of one of numerous specific statutory exceptions.[19] For example, a medical director agreement between a hospital and a referring physician must meet the specific requirements of Stark's personal services exception, which include a signed writing that covers all services provided by the physician, a term of at least one year, and compensation that is set in advance, is fair market value (FVM), and does not take into account the volume or value of referrals generated between the parties.[20] If the arrangement does not meet all of these requirements, the healthcare provider could face penalties of $15,000 per claim, treble damages, and/or potential exclusion from Medicare/Medicaid.[21]

In today's fast-paced healthcare world, agreements that fail to meet all of these specific requirements, especially the signature requirement, are not rare. But until the ACA, in-house counsel did not have a clearly established avenue through which to resolve such technical Stark violations, resulting in a case-by-case approach to such issues. In-house counsel historically would choose from a variety of options—making unsolicited refunds of "tainted" claims to CMS, disclosing through the HHS Office of Inspector General's (OIG's) self-disclosure protocol,[22] negotiating a settlement with OIG or the U.S. Attorney or, despite the fact that Stark is a strict liability statute, assuming the risk.

Section 6409 of the ACA changed these options when it mandated that CMS create a separate Stark self-disclosure protocol.[23] Established and implemented on September 23, 2010, the Medicare Self-Referral Disclosure Protocol (SRDP) was intended to facilitate the resolution of matters that, in the disclosing party's reasonable assessment, are actual or potential Stark violations. The ACA also granted the Secretary of HHS authority to reduce amounts due and owing for actual or potential Stark violations disclosed under the SRDP.[24] Nowhere in the protocol were allowances made, however, for "technical" Stark violations.

Until recently, we all have wondered whether the SRDP and the Secretary's newfound settlement authority would provide in-house counsel with comfort regarding those agreements that violate Stark only because of a lack of a signature that was not caught in time to meet Stark's applicable grace periods. As of the date of this article, CMS has entered into thirteen settlements under the SRDP, amounting to a total of more than $1.3 million.[25] The settlements range from $4,500 to $579,000, and all seem reasonable based on the very sparse amount of information provided by CMS. But the settlements still leave in-house counsel wondering. What is the difference between the settlement amounts and the providers' potential statutory penalties? How many other providers are taking advantage of the SRDP? How many disclosures currently are being submitting to CMS under the SRDP? How many disclosures were referred by CMS to OIG for prosecution under the Anti-Kickback Statute?

It will take time before trust can be built around the SRDP. While we wait for this trust to build, in-house counsel must choose how best to deal with Stark violations, whether deemed technical or not. Preventive measures may result in the best night's sleep for in-house counsel. In-house counsel should focus on the enhancement of internal policies and procedures with additional Stark approval requirements (including chief executive officer, general counsel, and chief compliance officer) and, as possible, the centralization of arrangements that may implicate Stark at the corporate office. Additionally, in-house counsel should provide widespread education on revised policies and procedures, and coordinate quarterly auditing of applicable arrangements with the compliance officer, with reporting to the corporate board.

Keeping Up With Audits

Related to the increased fraud and abuse enforcements above, the federal government also is increasing its audit activity. Between Recovery Audit Contractor audits, OIG audits, Zone Program Integrity Contractor audits, and HHS Office for Civil Rights (OCR) audits, government scrutiny is increasing and requires more resources than most in-house counsel have available on a regular basis. With regard to privacy and security, federal and state regulators are now armed with new power under the Health Information Technology for Economic and Clinical Health Act (HITECH Act)[26] and thus are expanding their enforcement activities. In 2011, OCR initiated a renewed focus on ensuring compliance across the healthcare industry with health information privacy laws. Not only has OCR hired an outside auditor (KPMG) to administer a nationwide Health Insurance Portability and Accountability Act (HIPAA)[27] audit performance program, but it has also already entered into significant settlements and levied heavy penalties.[28]

This increased scrutiny is happening at the same time that HIPAA compliance is becoming more complicated. Social media adds new challenges for in-house counsel, and hacker activities are on a steep rise. This past August, hackers struck a small medical practice in suburban Chicago, encrypted the facility's digital medical records, and then demanded ransom payment in exchange for allowing the facility to regain access.[29] Such stories are becoming more frequent, and in-house counsel must concern themselves not only with securing patient data from unlawful access, use, or disclosure, but also with backing up data to avoid such new challenges to the security of their health information.

Whistleblowers and Personal Accountability

There is no doubt that the healthcare climate has changed. In addition to keeping up with regulatory and enforcement changes, in-house counsel also have to worry about an expansion of potential whistleblowers and personal accountability. The ACA now makes it easier for an individual to qualify as an "original source" of underlying information in qui tam actions.[30] The ACA further expands whistleblower protections under the Fair Labor Standards Act. The result is an all-time high number of qui tam cases, along with an increased paranoia among in-house counsel regarding possible whistleblowers. In fact, whistleblowers earned a record-breaking $532 million in 2011.[31]

Just about anyone can be a whistleblower—disgruntled employees, competitors, former compliance officers—so there is a new urgency in responding quickly and effectively to discourage whistleblowers. This is especially true because the federal government not only is taking a closer aim at providers, but it is also targeting healthcare executives, including in-house counsel. With a new focus on personal responsibility, the federal government has promised to pursue individuals responsible for illegal conduct as vigorously as companies. In March 2011, Inspector General Daniel Levinson stated that "by excluding the individuals who are responsible for the fraud, either directly or because of their positions of responsibility in the company that engaged in the fraud, we can influence corporate behavior without putting patient access at risk."[32]

For instance, in *United States v. Stevens*,[33] the defendant, former GlaxoSmithKline (GSK) Associate General Counsel Lauren Stevens, was indicted based on her involvement in responding to a U.S. Food and Drug Administration (FDA) inquiry to GSK regarding possible off-label marketing of Wellbutrin SR for weight loss and obesity. In response to the FDA inquiry, Stevens sent six substantive letters and provided documents to the FDA between December 2002 and November 2003. The indictment charged her with two counts of obstruction of justice and four counts of false statements, alleging that GSK's letters to FDA contained false statements and that the document production to FDA was incomplete. Although ultimately acquitted, Stevens' indictment and prolonged involvement in this case was enough to make any in-house counsel take notice. No matter how long you have worked in healthcare, it will always be troubling to see your name individually listed as a defendant in any lawsuit against your organization.

Prescription for a Good Night's Sleep

So how can in-house counsel get a good night's sleep? The current healthcare climate and the government's increased scrutiny is, unfortunately, a fact of life. Despite arguments surrounding the constitutionality of healthcare reform, there does not seem to be much dispute that the fraud and abuse initiatives built into the ACA have been viewed as successful. Thus, the best medicine for in-house legal counsel is to ensure that your organization has implemented an effective compliance program that can keep up with the changes.

OIG has published a series of guidance documents for various segments of the healthcare industry, including hospitals, nursing facilities, physician practices, and pharmaceutical manufacturers.[34] The 2010 Federal Sentencing Guidelines also provide a federal model for how to structure governance and compliance programs.[35] Factors that underscore all of these compliance program models are:

- Written policies and procedures;
- Effective training and education;
- Effective lines of communication;
- Internal monitoring and auditing;
- Enforcement through well-publicized disciplinary procedures; and
- Prompt response to detected problems, with corrective action.

Additionally, any effective compliance program should be based on a current risk-based agenda and closely monitored by a designated compliance officer who has adequate resources and access to corporate issues. In-house counsel should pay close attention to OIG's work plan, published each year, as notification of OIG's ongoing and new activities.[36] To ensure Stark compliance, most arrangements should be accompanied by FMV determinations. With regard to HIPAA, in-house counsel should note that OCR has sent notifications to covered entities for audits this year, and recommends that all covered entities conduct regular program reviews and updates. Ongoing policy review and revision is a compliance requirement. At the end of the day, an ounce of prevention ultimately is worth a pound of cure.

1 Health Care Fraud Prevention and Enforcement Action Team, *information available at* www.stopmedicarefraud.gov/heattaskforce/index.html.
2 United States Dept. of Health & Human Services., News Release: "Health care fraud prevention and enforcement efforts recover record $4 billion; new Affordable Care Act tools will help fight fraud" (Jan. 24, 2011).
3 Trac Reports, Inc., "Record Number of Federal Health Care Fraud Prosecutions Filed in FY 2011."
4 United States Dept. of Justice, FY 2013 Budget Request, *available at* www.justice.gov/jmd/2013factsheets/health-care-fraud.pdf.
5 The Patient Protection and Affordable Care Act (hereinafter referred to as ACA), Pub. Law 111–148 (March 23, 2010), *available at* www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf.
6 The Fraud Enforcement and Recovery Act (hereinafter referred to as FERA), Pub. Law 11-21 (May 20, 2009), *available at* www.gpo.gov/fdsys/pkg/PLAW-111publ21/html/PLAW-111publ21.htm.
7 42 U.S.C. § 1320a-7k(d).
8 ACA § 6402(a).
9 Centers for Medicare & Medicaid Services, Medicare Program; Reporting & Returning of Overpayments, 77 Fed. Reg. 9179 (Feb. 16, 2012) (proposed rule), *available at* www.gpo.gov/fdsys/pkg/FR-2012-02-16/pdf/2012-3642.pdf.
10 *Id.* at 9182.
11 *Id.*
12 *Id.*
13 *Id.*
14 *Id.*
15 31 U.S.C. § 3731(b)(1).
16 42 C.F.R. § 482.24(b)(1) (hospitals).
17 42 C.F.R. § 1003.132.
18 42 C.F.R. § 405.980(b). There is no corresponding proposed amendment to the NPR determination regulatory reopening period, which remains three years.
19 Section 1877 of the Social Security Act; 42 U.S.C. § 1395nn.
20 42 C.F.R. § 411.357(d).
21 42 U.S.C. § 1395nn(g)(1-5).
22 Office of Inspector General, Publication of OIG's Provider Self-Disclosure Protocol, 63 Fed. Reg. 58399 (Oct. 30, 1998); *available at* http://oig.hhs.gov/compliance/self-disclosure-info/index.asp.
23 CMS Voluntary Self-Referral Disclosure Protocol, OMB Control No. 0938:1106, *available at* www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/Self_Referral_Disclosure_Protocol.html.
24 *Available at* www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/downloads/CMS-SRDP-Report-to- Congress.pdf.
25 *Available at* www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/Self-Referral-Disclosure-Protocol-Settlements.html.
26 Health Information Technology for Economic and Clinical Health Act, §§ 13401, 13404.
27 Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-101, 45 C.F.R. pts. 160,164, subpts. A, C.
28 *Available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.
29 *Available at* www.bloomberg.com/news/2012-08-10/hackers-encrypt-health-records-and-hold-data-for-ransom.html.
30 31 U.S.C. § 3730(e)(4)(B).
31 *Available at* www.reuters.com/article/2012/01/06/us-doj-whistleblowers-idUSTRE80528G20120106.
32 Testimony of Daniel R. Levinson, Inspector General, Office of Inspector General, Department of Health and Human Services on Preventing Health Care Fraud: New Tools and Approaches to Combat Old Challenges before Committee on Finance, United States Senate (March 9, 2011).
33 *United States v. Stevens,* No. 10-CR-0694 (D. Md. Mar. 23 2011).
34 *Available at* http://oig.hhs.gov/compliance/compliance-guidance/index.asp.
35 *Available at* www.ussc.gov/Guidelines/2011_guidelines/index.cfm.
36 *Available at* http://oig.hhs.gov/reports-and-publications/workplan/index.asp.

AHLA WEBINARS WILL SOON BE AVAILABLE ON DEMAND!!!

We know what you're thinking.

NO! You won't be able to view old episodes of your favorite reality shows and sitcoms on our website...but you WILL be able to earn CLE credit by purchasing past AHLA webinars at your leisure.

For more information, or to be notified when we begin piloting these on-demand offerings, email pgs@healthlawyers.org.

...stay tuned.

AMERICAN
HEALTH LAWYERS
ASSOCIATION

1620 Eye Street, NW
6th Floor
Washington, DC 20006-4010