HOSPICE EndNotes
for the North Carolina Hospice Community from Poyner Spruill LLP

JUNE 2010

Using Cleaning/Maintenance Services or Consultants

Are These Relationships Putting Your Company at Unnecessary Risk?

By Jennifer Parser

An independent contractor or subcontractor whose illegal workforce is on your premises creates an area of vulnerability where Immigration Customs and Enforcement (ICE) can apply sanctions against your company. ICE can deem these workers to be your employees under two circumstances: (1) there are indications of an employer/employee relationship, extremely broadly defined by the amount of control your managers exercise over these workers or (2) you have actual or "constructive" knowledge that the independent contractor's workforce is illegal.

Independent Contractor or Employee?
In assessing the risk of ICE sanctions through your independent contractor, your treatment of your independent contractor's workforce is determinative. Broadly stated, an independent contractor can be deemed to be your employee based upon the amount of control you exercise. A true independent contractor performs work according to its own means and methods and is subject to your control only as to results. A few factors indicating a true independent contractor relationship are that it offers its services to the general public and that it works for several clients simultaneously, supplying its own tools or materials and independently determining the order in which it performs its work. To illustrate, let us look at two common types of independent contractors you might have on your premises, so that we can help you and your company be as ICE-proof as possible in both situations.

Using an Outside Cleaning or Maintenance Service?
To avoid liability based on knowledge that cleaning or maintenance workers are illegal, your HR department should not review these workers' I-9s. Reviewing the I-9s would give your organization either actual or constructive knowledge of a potentially illegal worker. Further, doing so may evidence an employer/employee relationship with the worker because this could be seen as a form of control you are exercising over him or her.

Knowing that the independent contractor's employees on your premises lack employment authorization can be considered by ICE to be harboring, a felony carrying a maximum of ten years' imprisonment and the greater of $250,000 in fines or twice the gain these workers afforded your company. Wal-mart agreed to a settlement with ICE of $11 million in penalties for turning a blind eye to a subcontractor that employed an illegal workforce to clean Wal-mart's premises.

At a minimum, there are several protective measures you can take if you use such independent contractors. Have your agreements with the independent contractor reaffirm the independent contractor relationship, confirm the legality of its workforce and provide indemnification in the event that you are targeted by ICE for any illegal workers on your premises. Note, however, that this protection may still not absolve your company from liability if the independent contractor's workforce is being supervised, controlled and otherwise treated by your managers as if they are your employees. It is therefore critical that you also train your managers to treat independent contractors and their workers as independent entities rather than as your employees.

What About Using Consultants?
The second common form of independent contractor relationship is the use of an outside consultant, as is frequently the case in the IT industry. In fact, it has become standard practice for an H-1B nonimmigrant visa holder to be sent by his or her employer, an IT consulting firm, to work on long term projects on a client's premises. These arrangements are coming under scrutiny by the United States Citizenship and Immigration Service (USCIS) for two reasons: not conforming to a true employer/employee relationship required to maintain H-1B visa status, and failing to meet local wage standards for the geographic location where the visa holder is actually working vs. the employer's location. While the USCIS has not yet determined that the company on whose premises the IT consultant's "employee" is working is actually that worker's employer, you do not want to be placed in a position of defending your lack of control over this consultant to demonstrate that he or she is not your employee. Instead, in addition to reaffirming in writing the independent contractor relationship with your IT consulting firm, you should require a certification that the individual on your premises, if an H-1B visa holder, is both the consulting firm's employee by US immigration law standards and authorized under both state and federal department of labor standards to work on your premises. Once again, do not treat this individual as your employee by exercising control or providing supervision.

Conclusion
Independent contractors perform valuable services for a company. Just be certain that their employees are not considered by either ICE or the USCIS to be your employees. Have experienced immigration counsel review any agreements you have in place, and impress upon your managers the proper way to treat these individuals.

If you have specific questions or other immigration-related concerns, please feel free to contact Jennifer Parser at jparser@poynerspruill.com or 919.783.2955. She is licensed in the state of New York and is not licensed in North Carolina.

The Patient Protection and Affordable Care Act and Its Impact on Hospice

By Mike Hale

The health care reform bill signed into law by President Obama on March 23, 2010, otherwise known as the Patient Protection and Affordable Care Act (PPACA), will have a broad impact on virtually all aspects of health care, with hospice being no exception. Since the implementing regulations to the PPACA have not yet been published, we do not know the specifics of how we will be expected to achieve its new requirements. However, we do know what Congress intends the end results to be. The impact on hospice providers can be defined in terms of quality, data collection, accountability, payment reform and access to care. Some of the more significant provisions of the PPACA, as applied to hospices, are summarized below.

Quality
Various reports by the Office of Inspector General (OIG) and the Medicare Payment and Advisory Commission (MedPAC) over the last few years have found that it is difficult to assess quality among hospices because there are no uniform quality data requirements. The PPACA will address this issue by requiring hospices to report on quality measures to be determined by the Secretary for the Department of Health and Human Services (Secretary) or face a 2% point reduction in their market basket percentage increase. The Secretary must publish the quality measures no later than October 1, 2012, and the reporting would begin in Fiscal Year 2014. Quality measure data will be made available to the public after the reporting hospice has an opportunity to review the data. While we do not know what will be included as quality measures, we should consider that the PEACE Project and AIM Project, both funded by CMS, will be potential sources.

The Secretary will also establish a hospice concurrent care demonstration program. This three-year demonstration project will allow Medicare hospice beneficiaries to simultaneously receive hospice care in addition to other Medicare-covered services and will evaluate whether patient care, quality of life and cost-effectiveness were improved. No more than 15 hospice programs from both urban and rural areas will be selected for this project.

Data Collection
Lack of available uniform data among hospices is also a concern of MedPAC. Even though we have seen a substantial increase in the amount of data collected on hospice claims and cost reports, we can expect to see additional data requirements later this year. Beginning no later than January 1, 2011, the PPACA requires the Secretary to collect additional data as appropriate to revise hospice payments. The specific data requirements will be made in consultation with MedPAC and may include cost and charge information, charitable contributions, and patient visits.

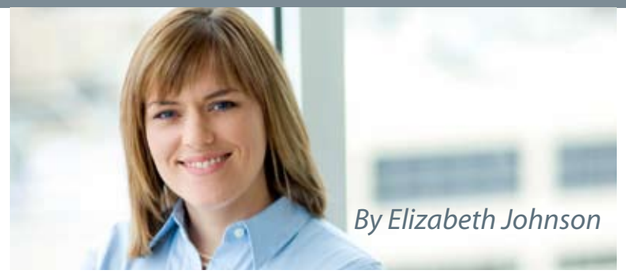
Accountability
MedPAC's recent recommendations regarding hospice recertification of terminal illness have also been included in the PPACA. Effective January 1, 2011, a hospice physician or nurse practitioner must have a face-to-face encounter with the hospice patient to determine continued eligibility prior to the 180th day recertification, and each subsequent recertification, and attest that such visit took place. In addition, the PPACA requires medical review of hospice patients with lengths of stay greater than 180 days for those hospice programs in

continued on Page 3

RALEIGH CHARLOTTE ROCKY MOUNT SOUTHERN PINES WWW.POYNERSPRUILL.COM
301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

Audits and Breaches and Fines, Oh My! – Part 2

Further progress along the HIPAA brick road



By Elizabeth Johnson

In last month's issue of *Endnotes*, we covered the "why" of HIPAA compliance. Now let's consider the "how." How exactly do you review your HIPAA privacy and security compliance program and ensure that all the requisite bases have been covered?

Know Your Obligations

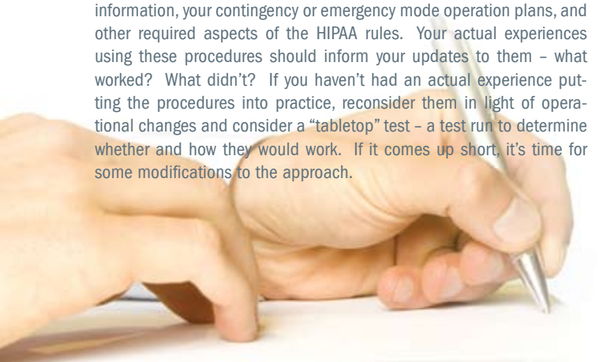
Your first step is to identify all your legal requirements. For privacy and security purposes, these are enumerated in the HIPAA Privacy, Security and Breach Notice Rules. You need to identify each requirement that must result in some "end product." Depending on the requirement, that could mean a documented policy or procedure, a set of security reminders, training programs, a complaint process, an incident response plan, etc. If you've never asked a lawyer to review your program to determine whether each of these end products is addressed, this might be a good time to consider that step.

Identify and Address Gaps

Once you have identified all the requirements for an end product, it's time to review your program to see if it actually consists of all those pieces. Is anything missing? Where are your gaps? Once you have found the gaps, you'll need to address them, and this may mean drafting a policy, conducting training, instituting a new procedure, or preparing some other "end product," depending on the requirement you are trying to address.

Test Your Program and Consider Lessons Learned

Assuming you have all the pieces in place, it's time to consider how well they actually work. If you have a complaint process in place (which is required), how well does it work? Has it ever been used? If not, should you test it to determine whether it would work? The same questions can be asked of your security incident response plan, your procedure to address individuals' requests for access and amendment of their information, your contingency or emergency mode operation plans, and other required aspects of the HIPAA rules. Your actual experiences using these procedures should inform your updates to them – what worked? What didn't? If you haven't had an actual experience putting the procedures into practice, reconsider them in light of operational changes and consider a "tabletop" test – a test run to determine whether and how they would work. If it comes up short, it's time for some modifications to the approach.



Security Rule Compliance

Security Rule compliance deserves some special consideration. Whereas Privacy Rule compliance is primarily administrative (implementation of policies and procedures), Security Rule compliance is one part administrative safeguards and two parts physical and technical safeguards. That means that covered entities have to take a multidisciplinary approach to compliance. When I assist clients in a Security Rule compliance review, I always ask to meet with their IT personnel or provider. You simply cannot assess compliance with this rule unless you ensure that the physical and technical security controls are in place. More than likely, you will have to explain the legal obligations to your IT staff and, through a series of discussions with them, determine whether their existing security measures, policies and procedures meet the rule's requirements. Very often, an existing security measure is appropriate but has not been documented. In those cases, the requirements are not met, due to the lack of documentation.

Another important aspect of the Security Rule is dealing with "addressable" implementation specifications. Covered entities may have an option not to implement those specifications denoted as "addressable," but only after they complete (and document) an assessment to determine whether the specification was reasonable and appropriate for the organization in light of the size, complexity and capabilities of the organization; the probability and criticality of the potential risks to information; the cost of implementation; and the organization's technical infrastructure. This process need not be daunting, and a legal review is often appropriate for completion of the task.

Business Associates

As a result of the HITECH Act, all your business associate agreements require an update (yes, it's required). More important, you need to make sure that your business associates are fully complying with the Security Rule, another new obligation imposed by the HITECH Act. Previously, your business associates' security measures needed only to be "reasonable and appropriate," which is a far cry from full compliance with the more than 60 specific safeguards outlined in the Security Rule. If they aren't complying, your business associates are putting your protected health information at risk. That risk is now greatly exacerbated by the breach notice obligations, which require covered entities to provide notification letters when security incidents are caused by their business associates. In other words, your business associate's security lapse could result in substantial notification costs and enforcement risks for your organization. These costs and risks are further magnified by the increased HIPAA penalties, audits and enforcement also implemented by the HITECH Act.

Paper the Problem

When the Office of Inspector General audited Atlanta's Piedmont Hospital on Security Rule compliance in March 2007, it gave Piedmont 10 days to respond to a list of 42 questions and requests. To comply with a request like that, you want to have all your compliance paperwork pulled together in a single location, fully organized and up-to-date in advance of receiving the inquiry. Once you determine that you have all the requisite pieces documented, get organized. At a minimum, that means collecting together all the following:

- All the requisite HIPAA privacy policies and procedures
- All the requisite HIPAA security policies, procedures, security plans, security reminders, documentation of access rights, etc.
- The requisite HITECH breach response procedures
- Notice of Privacy Practices
- Log of HIPAA training
- Accounting of disclosures for the past six years
- Hybrid entity designation (if applicable)
- Log of security incidents
- All of your organization's business associate agreements

Elizabeth Johnson's practice focuses on privacy, information security and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

PPACA...

continued from Page 1

which the number of such cases exceeds a percentage to be specified by the Secretary. This requirement is also effective January 1, 2011.

Payment Reform

Beginning in Fiscal Year 2013 and continuing through 2019, the annual market basket increase (MBI) will be reduced by a productivity adjustment that, for planning purposes, is often estimated to be around 1.3%, plus an additional 0.3% for hospices. This approximate 1.6% reduction to the MBI will be in addition to the Budget Neutrality Adjustment Factor reductions that are to continue for the next six years. In addition, the PPACA requires the Secretary, no earlier than October 1, 2013, to "...implement revisions to the methodology for determining the payment rates for routine home care and other services... which may include adjustments to per diem rates that reflect changes in resource intensity in providing such care...." The Secretary shall consult with hospice programs and MedPAC in regard to such payment revisions.

Access

The PPACA also allows concurrent care for children, as defined by state law, who are enrolled in Medicaid or the Children's Health Insurance Program to receive hospice services without waiving other coverage for the treatment of their illness.

We can expect to see implementing regulations beginning within the next few months that will provide us with the road map of how we are to achieve the PPACA's many new requirements for hospice agencies. Stay tuned to future editions of *Hospice EndNotes* as we discuss the specifics of the new regulations as they are published.

Mike Hale advises clients on a variety of regulatory, contractual and operational issues in hospice, home care and long term care settings. Mike may be reached at 919.783.2968 or mhale@poynerspruill.com.

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