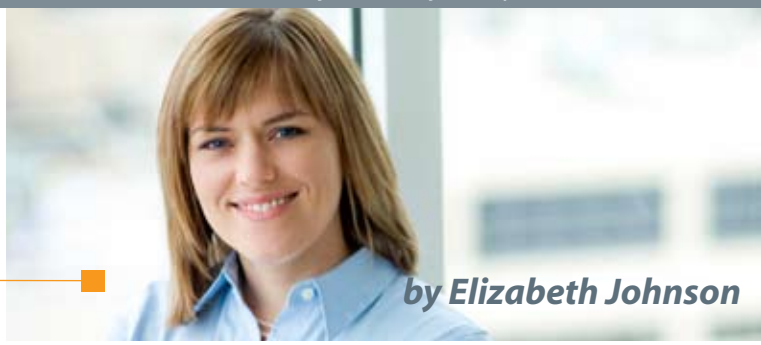
MAY 2010

SHORTS ON LONG TERM CARE

for the North Carolina LTC Community from Poyner Spruill LLP

Audits and Breaches and Fines, Oh My! — Part I

It's time to make sure your HIPAA privacy and security compliance program has a heart



by Elizabeth Johnson

Have you ever had that nagging feeling that you needed to take care of something, but you just didn't have time so you let it go, probably for too long? I usually feel that way about two things: exercise and yard work. Some HIPAA-covered entities feel that way about compliance with the HIPAA Privacy and Security Rules. They are cumbersome, dense, and difficult to fully implement. And even if you have implemented policies and procedures to address each requirement, your compliance program can't be a tin man. To effectively reduce risk of compliance problems and security incidents, you need to make sure the program actually functions, has been meaningfully implemented, and is refreshed periodically to address any compliance gaps created by changes in the law and your own operations. Breathing life into your compliance program takes real work, but doing so will have tangible rewards as the program becomes a living part of your organization's daily functions.

If you don't feel confident about your organization's HIPAA privacy and security compliance, now is a good time to undertake a refresher. Here are a few reasons why.

"Meaningful Use" Incentives

Let's start by discussing the carrot in this bunch. As part of the 2009 economic stimulus package, CMS was directed to provide incentive payments to eligible professionals and hospitals that make "meaningful use" of electronic health record technology and participate in Medicare and Medicaid. As part of their proposed rule to implement this requirement, CMS identified a series of "health outcome policy priorities" to be met, including "ensur[ing] adequate privacy and security protections for personal health information." As a Stage 1 measure, eligible professionals and hospitals must "[c]onduct or review a security risk analysis...and implement security updates as necessary." If you comply with the HIPAA Security Rule, you will have met this Stage 1 requirement.

Breach Notification

If meaningful use incentives are the carrot, the rest of the motivators on this list are sticks. Breach notification is a very big stick. In August 2009, as directed by the HITECH Act, HHS issued an interim final rule requiring covered entities to notify affected patients when their protected health information is the subject of a security breach. Whether it's a lost laptop containing medical records, a misdirected fax or an intrusion by a hacker (or an unauthorized employee), these incidents may require that your organization send a letter to each person whose protected health information was affected, noting what happened, when it happened, and what you are doing to address it. You also have to notify HHS, and possibly the media. Existing notification laws at the state level have shown that sending these letters often prompts a government investigation of the organization's privacy and security compliance, and sometimes spawns lawsuits by affected individuals. Ensuring compliance prior to one of these events can mitigate their impact, in part by minimizing the risk of a government enforcement action and as a defense to a potential lawsuit.

Government Enforcement

For several years now the Federal Trade Commission and state regulators have been taking enforcement actions against organizations that report security breaches. The pattern goes as follows:

1. Organization experiences a security incident affecting personal information
2. Organization sends a letter to affected individuals, as required by state law, describing what went wrong
3. Government regulator receives a similar notice (often required under state law) or reads about the incident in the press
4. Notice letter prompts regulator to investigate whether organization's security was adequate in light of the incident
5. Regulator alleges that incident demonstrates inadequate security, and charges organization with an unfair trade practice pursuant to the federal or state unfair and deceptive trade practices statute it enforces

In February 2009, HHS joined the party, taking a joint enforcement action with the FTC against CVS Pharmacy following multiple reports that employees disposed of prescription information in dumpsters. The result was a settlement with both agencies, including a $2.25 million payment by CVS and an agreement to implement a comprehensive, written information security program with oversight from HHS, as well as submitting to audits of compliance with that plan biennially for 20 years. This action predated the HITECH Act and HHS's breach notification rule, which now require covered entities to self-report the type of security incident that led to the action against CVS.

(continued on page 3)

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

Using Cleaning/Maintenance Services or Consultants: Are You Putting Your Company at Unnecessary Risk?

By Jennifer Parser

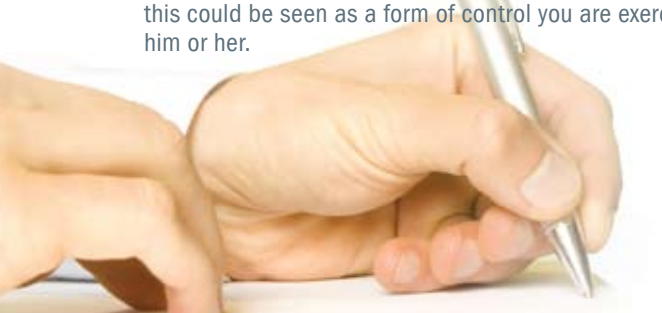
Using an independent contractor or subcontractor whose illegal workforce is on your premises creates an area of vulnerability where Immigration Customs and Enforcement (ICE) can apply sanctions against your company. ICE can deem these workers to be your employees under two circumstances: (1) there are indications of an employer/employee relationship, extremely broadly defined by the amount of control your managers exercise over these workers or (2) if 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 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 and assist you and your company to be as ICE-proof as possible in both situations.

Using an Outside Cleaning or Maintenance Service?

To avoid liability based on knowing 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 or having constructive knowledge 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. Walmart 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 Walmart'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 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 through 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: for not conforming to a true employer/employee relationship required to maintain H-1B visa status and for 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 company's employee, 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, require a certification that the individual on your premises, if an H-1B visa holder, is both its 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 how 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.

Ken's Quote of the Month

"Our truest life is when we are in our dreams awake."

Henry David Thoreau

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

Audits... (*continued from page 1*)

Increased Penalties

The HITECH Act was just full of motivators to compel HIPAA privacy and security compliance. The same statute that brought you breach notification and additional privacy and security obligations also increased the penalty amounts HHS can seek for noncompliance. Whereas penalties were previously capped at $25,000 for multiple violations of the same provision in a single calendar year, they are now capped at $1.5 million.

Mandatory Audits and State Enforcement

In case breach notification and increased penalty amounts were insufficient incentive to comply, the HITECH Act also made periodic HIPAA audits by HHS mandatory and authorized state attorneys general to enforce HIPAA. Wasting no time (and having announced days earlier his intention to seek the Senate seat soon to be vacated by Chris Dodd), Connecticut Attorney General Richard Blumenthal in January became the first state AG to exercise his newfound HIPAA enforcement authority. Blumenthal filed suit against Health Net, which allegedly lost a portable disk drive containing unencrypted protected health information, social security numbers and bank account numbers of approximately 1.5 million past and present enrollees, including 446,000 Connecticut residents. The suit alleges that Health Net failed to notify affected individuals for approximately six months following discovery of the incident. Mr. Blumenthal already is engaged in a second HIPAA-related action, investigating an alleged breach of medical records at Griffin Hospital in Derby, Connecticut, where a radiologist allegedly accessed patient information and used it to promote his services offered at another medical facility.

Threats to Medicaid and Medicare Reimbursement

In case you were thinking that the worst-case scenario in a breach situation is allegations of HIPAA violations and a potential fine, let's consider the case of Wentworth-Douglass Hospital in Dover, New Hampshire. That facility has been the subject of an investigation by the New Hampshire attorney general following an alleged breach of patient medical records. What's different about this investigation is that CMS joined the investigation, sending surveyors from the New Hampshire Department of Health and Human Services to examine not only privacy and security issues, but also patients' rights and quality assurance in order to determine whether the facility meets the "conditions of participation" for reimbursement by Medicaid and Medicare.

With all these compelling reasons to revisit your HIPAA privacy and security compliance, you may be wondering where to start. In next month's issue of Shorts, we'll provide a road map to reevaluating HIPAA compliance. In the meantime, our attorneys frequently assist covered entities of all shapes and sizes in implementing HIPAA privacy and security compliance programs. If you have any questions about this article or need assistance with HIPAA or the new HITECH requirements, please contact us today.

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

Social Media: A Blessing or a Curse for Providers?

By Kim Licata

Twitter, Facebook, LinkedIn, YouTube...use of social media is growing by leaps and bounds. You can't go a day without hearing about social media, whether it's on the television or in a magazine or you are actively using social media. Health-related social media is no different, and for many providers, the potential value of getting their information online is enormous. Before bravely exploring the social media frontier, what do you need to know? After all, it's a jungle out there!

Employment Issues

Social media challenges both employers and employees. Even if an employer prohibits social media, either in part or whole, at work, employees still frequently post comments, stories, and images that pertain to work or their employer in their off-hours. An inappropriate post can create problems (legal or otherwise) for both employers and affected employees. Inappropriate posts (or pictures) may be publicly searchable, leading to embarrassing incidents. Given the risks, as well as the potential benefit of positive stories shared about a company, employers should develop policies on social media use, appoint appropriate "watchdogs," and monitor compliance with the policy.

Privacy

Health care providers know all about privacy and security in light of HIPAA and HITECH. With social media, new threats arise, including claims for invasion of privacy based on posted stories and images. Common sense cannot be left at the door with social media! Think before you post. What may be amusing to a small number of "friends" may not be acceptable to the general public. Educate (and guide) social media users as part of your social media policy. A useful suggestion is to ask employees, "Would you want your posted information to appear on the front page of the *New York Times*?" If not, then don't post it, chances are the information is inappropriate (at least to someone).

Patients and Family Members

Recommendations from patients and their families are critical to the success of a provider. Happy patients mean happy family members. In the context of social media, positive posts and images may make all the difference in selection of a health care provider. Social media can highlight the compassion and positive interventions of hospice in a family's life (or the absence of these things). Hospice providers may consider using a "fan" page, a blog, or other social media group to gather positive stories. Statistics show that a third of Internet users are over age 45, and the fastest growing group of social media users is age 54 or older.

Regulatory Issues

All health care providers are heavily regulated in how they conduct their business, advertise for their services, and provide care. Federal and state agencies, such as the Federal Trade Commission and state attorneys general, analyze statements made in marketing and communications about provider services to protect the public. Other agencies—like the Centers for Medicare & Medicaid Services and the Office of Inspector General—review payment arrangements for services under fraud and abuse laws and regulations. Payment terms, incentives, and advertisements for services can appear in social media. Such information must be reviewed prior to posting for regulatory compliance.

You need to discuss social media so that you can set clear policies, expectations, and boundaries with your staff and patients. To further this discussion, work with legal counsel (and other appropriate consultants) to maximize the benefits of social media while minimizing any potential liabilities. Don't be scared of social media. Look for opportunities to enhance your business with positive social media use.

Kim Licata has advised health care providers and facilities on regulatory and compliance issues for over 13 years. She may be reached at klicata@poynerspruill.com or 919.783.2949.