# Issues & Updates

Legal and Business Advice for Physicians and Dentists since 1970

Fall 2015

The Health Care Group®

Sister Company of The Health Care Group

Health Care Law Associates, P.C.

## HIPAA: Is Your Practice Ready for Phase Two Audits?

By: Jennifer B. Cohen, JD

According to a recent KPMG survey, four out of five surveyed executives of health care providers and insurers admitted that their information technology has been compromised by cyber-attacks at least once in the last two years. More worrisome is that only half of these executives believe that they are not adequately prepared for future attacks.

It is also noteworthy that the survey respondents were larger entities, with revenues of at least $500 million per year. If larger entities are still not adequately pro-

*(Continued on page 2)*

## Is Your Practice Protected Against Bad Behavior By Employees? Not always, but make sure you understand some basics to lessen your risk.

By: Joseph W. Gallagher, JD, LLM

As a practice owner or administrator, you recognize that your doctors and staff are a source of tremendous skill, energy and capacity, delivering the best care to your patients. On the flipside, employees occasionally act badly or even illegally, or they make errors in judgment or conduct and can be *perceived* as insensitive, offensive or oppressive by fellow employees. Improper behavior, mistakes in judgment and even the perception of being wronged can become legal nightmares for the practice entity and its owners. Human resource consultants and employment lawyers consistently advise their clients to be proactive when it comes to risk management. Risk manage-

*(Continued on page 3)*

### Inside this Issue

HIPAA: Is Your Practice Ready for Phase Two Audits? ..... 1

Is Your Practice Protected Against Bad Behavior By Employees? Not always, but make sure you understand some basics to lessen your risk..... ..... 1

Does Your Practice Need a Practice Retreat? ..... 6

Practice Sales: Feedback from the Trenches ..... 12

### Attorneys and Consultants

Daniel M. Bernick, JD, MBA
dbernick@healthcaregroup.com

Joseph W. Gallagher, JD, LLM
jgallagher@healthcaregroup.com

Mark E. Kropiewnicki, JD, LLM
mkrop@healthcaregroup.com

Jennifer B. Cohen, JD
jcohen@healthcaregroup.com

# HIPAA: Is Your Practice Ready for Phase Two Audits?

*(Continued from page 1)*

tected, how much more vulnerable are smaller entities, such as independent physician practices?

The problems faced by smaller practices are illustrated by a recent settlement announced by the Department of Health and Human Services ("HHS") in September. The settlement was made by a 17 doctor private group named Cancer Care Group, P.C. for $750,000.

On August 29, 2012, Cancer Care reported to HHS's Office for Civil Rights ("OCR") (the agency that enforces HIPAA) that a bag had been stolen from an employee's car containing the employee's computer as well as unencrypted backup media. The computer and media contained large amounts of unsecured electronic protected health information ("e-PHI"), including names, addresses, dates of birth, Social Security numbers, insurance information, and clinical information of approximately 55,000 current and former patients. To settle the potential HIPAA fines, the group agreed to pay $750,000 and to implement a stringent corrective action plan. The practice will face oversight by government monitors for years to come.

With the second round of audits coming, all covered entities and business associates should be prepared. The audits are intended to be educational. However, they could result in a referral to the OCR Regional Office responsible for your Practice, and the resulting OCR investigation or compliance review could result in substantial penalties.

In 2011 and 2012, OCR conducted its first HIPAA audit of physician practices and other providers. In this "Phase One" audit, OCR chose 115 covered entities as a sample representative of all healthcare providers, health plans, and healthcare clearinghouses. Phase One focused on the Privacy Rule (specifically practices' Notice of Privacy Practices, rights to request privacy protection for PHI, access of individuals to PHI, administrative requirements, uses and disclosures of PHI, amendment of PHI, and accounting of disclosures), the Security Rule, and the Breach Notification Rule. Results showed that a large percentage of covered entities are not in compliance; the audits revealed that many practices do not conduct a thorough risk analysis and, when a breach is discovered, do not comply with the Breach Notification Rule.

Now, OCR is gearing up for "Phase Two". OCR will audit approximately 150 covered entities and 50 business associates for compliance with the Security Rule, 100 covered entities for compliance with the Privacy Rule, and 100 covered entities for compliance with the Breach Notification Rule.

Phase Two audits will consist largely of desk (that is, off-site) audits; however, OCR will be conducting some comprehensive audits also.

With the second round of audits coming, all covered entities and business associates should be prepared. The audits are intended to be educational. However, they could result in a referral to the OCR Regional Office responsible for your Practice, and the resulting OCR investigation or compliance review could result in substantial penalties.

Gone are the days when practices can just document a risk analysis and mitigation steps. OCR is expecting to see your HIPAA Compliance Program in action – what are your Practice's policies and procedure? How is your Practice responding to breaches? Is your Practice's HIPAA Compliance Program actually in place and effective? Now is the time to take a close look at your program and decide – is it sufficient to mitigate the risk of a HIPAA violation? Is it sufficient to guide your Practice in responding to a potential HIPAA breach? Is it sufficient to withstand the scrutiny of OCR?

Phase Two audits are coming whether you are ready or not…so start preparing now! Here are some things to keep in mind.

*(Continued on page 3)*

## Is Your Practice Protected Against Bad Behavior By Employees? Not always, but make sure you understand some basics to lessen your risk.

*(Continued from page 1)*

ment principles tell us that you must have sound defensive policies in place to preempt (or at least minimize) exposure for the bad actions of an individual employee.

In today's environment, two exposure areas come immediately to mind: (1) harassment and (2) activities utilizing electronic communications such as e-mail or social media. This article examines these topics and presents some guidelines for disarming behavioral time bombs that can turn into lawsuits.

**HARASSMENT**

You may wonder why in the world you should get worried if a "bad apple" shoots off a derogatory comment in the breakroom or quiets a staff meeting with a raunchy joke. There are a couple of reasons. First, your practice is a "deep pocket" and people will sue at the drop of a hat these days – that's an unfortunate

*(Continued on page 5)*

## HIPAA: Is Your Practice Ready for Phase Two Audits?

*(Continued from page 2)*

**Oversight**

For every finding and observation cited in OCR's Phase One audit reports, a "cause" was identified. The most common cause, across all entities, was that the entity was unaware of the requirement. Make sure your designated Privacy Officer is setting aside time on a regular basis to monitor HIPAA developments and respond appropriately.

Your Practice should also have a Security Officer (can be the same person as your Privacy Officer). The Security Officer needs to make sure that PHI cannot be viewed, tampered with, or stolen, which is mainly accomplished by the implementation of the administrative, physical, and technical safeguards outlined in your Practice's policies and procedures.

**Practice-Wide Risk Assessment**

Your HIPAA Compliance Program should be tailored to the specific needs of your Practice, as determined by your practice-wide risk assessment. Have you conducted a risk assessment? If not, you can use HHS's online risk assessment tool, available at: https://www.healthit.gov/providers-professionals/security-risk-assessment.

**Policies and Procedures**

Policies and procedures provide step-by-step instructions, designed to direct your Practice to comply with the HIPAA Rules. The Health Care Group® offers a template program for use by medical practices (see our website www.thehealthcaregroup.com.) This template incorporates the changes made by the Final Omnibus Regulation in early 2013. However, to be maximally effective, this template should be customized to your Practice, based on your internal risk assessment.

**Adequate Safeguards**

Both the Privacy and Security Rules require that adequate administrative, technical, and physical safeguards be in place for the protection of PHI, in any form. Of particular concern are technical safeguards relating to access to technology and the protection of e-PHI.

In today's health care environment, laptops, tablets, smartphones, thumb drives, and other mobile devices are commonplace. E-PHI

*(Continued on page 4)*

# HIPAA: Is Your Practice Ready for Phase Two Audits?

*(Continued from page 3)*

shared on mobile devices is especially vulnerable to attacks due to potential hacking and risk of loss and theft. Your policies and procedures should address how you are protecting e-PHI and other sensitive information on both corporate-owned and personally-owned devices. There should be policies in place for the use of mobile devices as well as the disposal of mobile devices when replaced. Employees should be trained on proper practices for storing and accessing e-PHI on mobile devices. Implement proper security mechanisms, including encryption. (Note that while encryption is merely an "addressable" requirement, it must be implemented if it is reasonable and appropriate.)

**Training and Education**

HIPAA training should be conducted for new employees as soon as possible after hire and should be conducted at least annually for all other staff. Are you still doing this? Maintain a culture of compliance. Note that documentation of attendance will serve as evidence of your Practice's commitment to the implementation of its HIPAA Compliance Program.

OCR is expecting to see your HIPAA Compliance Program in action – what are your Practice's policies and procedure? How is your Practice responding to breaches? Is your Practice's HIPAA Compliance Program actually in place and effective? Now is the time to take a close look at your program and decide – is it sufficient to mitigate the risk of a HIPAA violation? Is it sufficient to guide your Practice in responding to a potential HIPAA breach? Is it sufficient to withstand the scrutiny of OCR?

**Auditing and Monitoring**

Your Practice should have a system for routine identification and self-evaluation of compliance risk areas, which will help to examine mechanisms for compliance and discover vulnerabilities that may not be evident through compliance investigations and reviews.

The upcoming audits will largely target provisions that were the source of a high number of findings during Phase One audits. Therefore, we recommend that you focus particular attention on the following areas during your internal audits, so that you are prepared for Phase Two audits:

- Privacy: Notice of Privacy Practices, right to request privacy restrictions, access to patient records, administrative requirements, and uses and disclosures of PHI;

- Security: risk assessment, implementation of addressable implementation specifications (implement them!), access management, security incident procedures, contingency planning and backup, workstation security, and mobile device security and destruction; and

- Breach Notification: risk assessment to determine whether notification is necessary as well as timeliness and method of notification (primarily to individuals).

**Incident Response**

A breach occurs when there is an impermissible use or disclosure of PHI. An impermissible use or disclosure is presumed to be a breach unless you can demonstrate that there is a low probability that the PHI has been compromised. Note that this standard is new and is a lower threshold than the prior Rule; therefore, many incidents that were not previously considered a breach now will be considered a breach. That means that, upon discovery (that is, when you knew or should have known that a breach took place), you must take action.

What will you do if you have a breach? We know what everyone thinks – "that will never happen to me" – but the reality is that virtually everyone will. You should have a response policy, which should discuss investigation and breach notification procedures.

The internal investigation should focus on the following: What PHI was involved? To whom was the disclosure made? Was the PHI actually used or acquired? Is there any way to mitigate the risk? Again, unless there is a low probability that the PHI has been compromised, you have notice

*(Continued on page 5)*

## HIPAA: Is Your Practice Ready for Phase Two Audits?

*(Continued from page 4)*

obligations, to the individual to the government, and even possibly to the media. It doesn't hurt to practice your incident response policy, so that you are prepared.

**Conclusion**

Remember – being prepared with a plan is only the first step; putting the plan into action is crucial. It is important that your plan for detecting and responding to HIPAA privacy and security issues evolves over time, as the regulations are updated. Be sure to consult with a lawyer for specific advice as it relates to your Practice or fact-specific scenarios. If you have any questions about HIPAA compliance, The Health Care Group, Inc. can help. Visit us at: www.healthcaregroup.com or call Jennifer Cohen at 800-473-0032 extension 3316.■

## Is Your Practice Protected Against Bad Behavior By Employees? Not always, but make sure you understand some basics to lessen your risk.

*(Continued from page 3)*

reality especially given that the practice may have little control over the alleged offensive occurrence. Second, there's this legal doctrine known as "respondeat superior," which is Latin for "let the master answer." Essentially, it means that an employer may be held liable for an act of the employee that is committed within the "scope of employment." Over the years courts have allowed a liberal view of "scope of employment." For example, even if an employee disobeys the employer's explicit instructions, and as a result causes injury, as long as the injury occurred while the employee was working, the employer may be found liable.

Workplace harassment is any unwelcome or unwanted conduct that is based on race, color, religion, sex (including pregnancy), national origin, age, disability, genetic information or any other characteristic or class protected by federal or state law. To be unlawful, the conduct must create an intimidating, hostile or offensive work environment to a reasonable person and where the offensive conduct becomes a condition of continued employment. This means an employee has no other alternative but to come to work each day and be subjected to the offensive conduct.

So really, what is harassment? First, the conduct must be unwelcome or unwanted. A person who is offended at work (the victim) need not verbally tell the offending employee (the offender) that the offender's conduct is unwarranted or unwelcome. Some people, when offended, do not say anything for a variety of reasons. They may be afraid to instigate further harassing conduct. They may be too upset to say anything to the offender, although they are then likely to tell someone else.

Next, the definition of harassment addresses conduct. It is very important to remember that offensive conduct need not be physical. It can be verbal or visual. For example, name calling or offensive jokes may give rise to harassment in the workplace. Offensive cartoons from the paper hung up in a co-worker's desk, a racial slur or a sexually explicit scene on an employee's screen saver may be harassment to a fellow employee who observes it. Obviously, unwanted or inappropriate touching may be sexual harassment.

Last, the definition of harassment states the conduct must be "based on race, color, sex, religion, national origin, disability, and/or age." That foundation lies in Title VII of the Civil Rights Act. This is why teasing someone for pink hair is not harassment. It is not harassment because it is not a basis on which you can

*(Continued on page 9)*

# Does Your Practice Need A Practice Retreat?

By: Mark E. Kropiewnicki, JD, LLM

In a group practice, planning necessitates the input of all the owners to construct a viable business plan. Issues need to be dealt with, differing views need to be discussed, compromises need to be made and a direction set for the future. This kind of interaction is usually done within the confines of the office, yet the typical daily disturbances of phone calls, staff interruptions and a steady stream of patients tend to make productive planning difficult, if not impossible. It is hard to concentrate on future planning when there are other more day-to-day issues to deal with on a much more immediate basis.

Because thorough planning is such an important aspect of managing a group practice, an off-site planning retreat is beneficial to practice owners and also to non-owner providers who will be important to the future of the practice either as future co-owners or as patient care providers. The group practice can benefit from input from its non-owner providers during portions of the retreat. Similarly, the practice administrator or office manager should also be invited for most, if not all, of the retreat.

Commercial businesses large and small devote a day or more regularly to structuring and planning the direction of the company. Group practices would be wise to follow the same business principles. It makes good sense.

**Location**

The retreat can be held at a number of different places, but we find that the best location is usually a convenient hotel away from the office and its distractions. Sometimes retreat sessions tend to start early and run late, so staying overnight often makes sense especially if your retreat starts Saturday and ends Sunday morning. Most hotels offer meeting room space and can serve meals and provide refreshments during breaks in the meeting room. Also, if you use a hotel on the weekend, you may get a price break since meeting rooms tend to be vacant on the weekends.

**The Facilitator**

One person should be assigned the task of moderating and facilitating the retreat. It is usually not a good idea to have any of the practice's regular advisors handle this job. The practice's regular advisors often will be too close to the practice or have vested interests in the final decisions. Thus, the practice would be better served to have them as participants in the retreat. A better idea would be to have a business person or outside consultant with no affiliation to the practice but who knows and understands group practices serve as the facilitator. The facilitator can be nonjudgmental when issues are discussed and can also help keep discussions on track. The facilitator's main job is to keep the group focused on the primary goals of the retreat. It is easier to do this when the facilitator comes from outside the circle of the practice and its regular advisors.

**The Agenda**

The first item for the retreat agenda should be to develop the practice's Mission Statement. Your practice needs to go beyond the typical statement "providing quality patient care to our patients." Consider what you mean by "patient care." Does this mean the practice's basic care services or does it mean specialized or other ancillary care services? Think also of how broadly the term "patients" should be defined for your practice. A good Mission Statement is usually one clear, concise sentence that describes what the practice intends to accomplish.

Next on the agenda should be to outline the practice's strengths and weaknesses. It is important to do this before planning the growth or addition of services, adding more doctors or other providers, branching out into additional locations, etc.

A good facilitator will have an agenda prepared in advance so each participant can study it and prepare their thoughts for a good discussion. The facilitator will probably circulate a question-

*(Continued on page 7)*

# Does Your Practice Need A Practice Retreat?

*(Continued from page 6)*

naire to everyone involved in the retreat ahead of time to assist the facilitator in planning the key issues for the retreat. It also focuses the participants on what will be covered.

**Reference Material**

It is also a good idea to bring along reference material for the retreat. Most facilitators will ask for most of this ahead of time anyway, so that he or she can "do their homework" before the retreat. The facilitator will likely want various practice/provider information relating to types of patients and patient volumes; surgical and other procedures performed and where; aged accounts receivable; provider productivity; gross charges, collected income, practice overhead expenses and income available to compensate the practice owners; payor information/volumes; and demographic information on your practice region (or in the area you plan to expand to).

**Brainstorming Session**

A free-flowing brainstorming session should be the next part of the retreat process, starting with a listing of potential business/practice development ideas. These might include internal growth, such as improving operating efficiency, expansion or improved utilization of current services and improved utilization of current facilities and resources. Another strategy to focus on is provider growth in general patient care, subspecialty patient care, and non-doctor provider care. Be certain to mention growth in other service areas as well, like ancillary services, side businesses and targeted patient expansion. This free-flowing session should list all of the recommendations, without judgment – the list will be culled down later. For now, however, everyone's thoughts and input is essential.

Once strategies have been laid out, evaluate them for how much they will accentuate the practice's and its providers' strengths and if weaknesses will be avoided. Do the new strategies have the potential to fulfill the practice's objectives, yet at the same time fit into the confines of the available resources (human, financial, capital)? Consider if the resulting plan is consistent with practice policies and your newly developed Mission Statement. Some of the ideas will fall by the wayside during this process, but they all should be considered.

**Documentation and Implementation**

Everything that is generated from the retreat should be documented in writing so there is a "game plan" for the future, with timelines if possible. In addition, having group members' ideas recorded will help them feel they have contributed to the discussion. You do not need or want a fancy, bound business plan that will sit on a shelf. You need a working document that should be referred to often as your practice changes and develops. It should function as a checklist to assure that you are still on target with your developed practice strategies.

**How Often?**

Practices typically schedule one large retreat every 12 to 24 months or perhaps two smaller sessions during that timeframe. Anything more than that is not needed. You need time for plans to be implemented, modified and retested. And, you need enough time between to maintain interest.

**Summary**

For the retreat to be productive, the discussions need to be open, with all participants actively contributing to the conversation. Encourage everyone to (using a clichéd expression) "think outside the box." Group members need to be willing to compromise and to actively listen to each other. With these rules in place, your retreat can be a valuable tool in making your practice more focused, more efficient, and more prepared for the future.■

# HCG UPDATES OSHA EXPOSURE CONTROL PLAN MANUAL TO INCLUDE AIRBORNE PATHOGENS

## Order Your Copy Today

The Occupational Safety & Health Administration (OSHA) estimates that 5.6 million workers in the health care industry and related occupations are at risk of occupational exposure to bloodborne pathogens such as HIV, HBV, and HCV. In order to protect their employees with a safe and healthful workplace, OSHA Bloodborne Pathogens Standard requires that employers implement an Exposure Control Plan for its worksites where any employee(s) have occupational exposure.

HCG's *Model Medical Practice OSHA Exposure Control Compliance Plan* is designed to help medical practices comply with the Bloodborne Pathogens Standard. It includes information as required by the Standard as well as necessary charts and forms. As updated, in August 2015, the *Model Plan* will now exceed the requirements of the Bloodborne Pathogens Standard by including additional important information about *airborne pathogens* and preventing the spreading of airborne illnesses.

The *Training Module* included with the Model Plan has also been updated with information regarding airborne pathogens. The updated *Training Module* will remind your staff of respiratory and coughing etiquette and will help to eliminate the risk of transmission of airborne illnesses such as the flu and tuberculosis.

# Is Your Practice Protected Against Bad Behavior By Employees?

## Not always, but make sure you understand some basics to lessen your risk.

*(Continued from page 5)*

claim discrimination; pink hair is not a "protected class" of persons, unlike race, color, sex, etc. Unlawful harassment is a form of discrimination that violates state and federal law. Be aware that some states extend the definition of a protected class to include many other areas such as sexual orientation, gender, marital status, ancestry, citizenship, and pregnancy.

**Harassment Policy**

If a harassment lawsuit is pursued, the employer can raise a valid defense to liability through demonstrating that it had an effective anti-harassment policy in place and took care to prevent and correct any such behavior and that the employee failed to take advantage of the employer's preventive or corrective opportunities. Your practice has a harassment policy in its employee manual, so it is protected as an employer, right? Unfortunately, this is not necessarily true. Simply having a policy does not absolve the practice of liability if harassment occurs at the office.

So, dust off your practice's employee manual, review the harassment policy, and redistribute it to the staff. Have each existing employee and new hires sign a statement acknowledging the employee has received and reviewed the manual and completed training on the subject. Yes, training. Provide training to your staff. This training is an opportunity to educate your staff on what is and what is not harassment and to counsel your staff about the complaint process an employee should use when he or she believes harassment has occurred.

Be particularly sure that that these rules are understood and followed by *supervisory* staff and managers (anyone with supervisory authority in the practice at any level). Employers will undoubtedly be held liable for the harassing actions of their supervisors if the conduct resulted in a "tangible employment action." For example, if a supervisor told an employee that the employee would be fired unless she tolerated the clearly inappropriate behavior, she protested and was then fired, the employer is liable. Why would the employer be liable if the employer had no knowledge of the supervisor's conduct? That is because the supervisor, acting as an agent of the employer, conditioned the employee's employment on going along with the harassment and then fired her when she declined. This is called "quid pro quo" and will always result in employer liability, even though the employer may have been unaware.

If the harassment did not result in a tangible employment action, the employer may not be liable. Keep in mind that a tangible employment action is not just termination. It may be demotion, failure to promote, or relocation to an undesirable work location. To escape or minimize liability, the employer must prove the following: (1) the employer exercised reasonable care to prevent and promptly correct any harassment (remember, we recommended dusting off the harassment policy and training your employees); and (2) the employee unreasonably failed to complain to management or to avoid harm otherwise. So clearly describe your policy and training and the complaint process for any person who believes he or she is a victim of harassment, train and inform employees to use the process. If that is done, the employer can raise this as a defense to liability.

Be aware that harassment can occur between non-supervisory employees, not just between employees and supervisors. Also, the victim can be anyone affected by the conduct, not just the person to whom the conduct is directed. For example, there could be two employees telling each other off-color jokes. Neither is offended. However, another co-worker overhears the jokes and is offended. This may be considered a hostile work environment.

*(Continued on page 10)*

## Is Your Practice Protected Against Bad Behavior By Employees? Not always, but make sure you understand some basics to lessen your risk.

*(Continued from page 9)*

Train your supervisors on how to react to complaints, how to conduct a proper investigation, how to document the steps taken, and the appropriate disciplinary process in the event harassment is substantiated. In educating and training your supervisory personnel, there are certain attributes and skills you want them to develop and exercise in day-to-day functions around the office – these are:

- *Never tolerate workplace wrongdoing;*
- *Become more diligent observers; and*
- *Encourage communication, listening and empathy.*

**PRACTICE-RELATED USE OF E-MAIL AND SOCIAL MEDIA**

This is a constantly-changing area of employment and privacy law, so initially it's important to know what is currently allowed (note that you should always check with your legal advisor about the specifics of your own practice situation and the particular laws of your own state).

First, the practice may monitor employee work-related emails on work devices and it is often in the practice's best interest to do so. You need to be aware of what is happening in the workplace, and monitoring work email is one of the best ways to find out. However, the rules are not entirely clear when it comes to monitoring the *personal* emails of employees that are accessed on work devices. The answer turns on whether the employee had a reasonable expectation of privacy in the personal account when it was accessed at work.

Second, the practice may monitor its employees' social media use as long as it does not violate any laws or other applicable rules. Thus, activity that an employee has chosen to make public can be viewed, but employers may not pressure an employee for a password to his or her social media account, or create a fake account in order to gain access, etc.

**The Practice May Be Exposed**

With both e-mail usage and the explosion of social media use, you need to evaluate your existing procedures to minimize the potential for legal liability. Just as a supervisor's sexual advance toward a subordinate can result in liability, so too can an employee's use of social media expose your practice *both inside and outside* your workplace. Examples of social media applications are LinkedIn, Facebook, Wikipedia, YouTube, Twitter, Yelp, Flickr, etc. - the list is ever-expanding. Employees using social media can defame your practice or your practice's competitors, they can disclose protected health information in violation of HIPAA or they can greatly increase the practice's exposure to discrimination or harassment charges and lawsuits.

**Employees Can Discuss Wages, Benefits and Working Conditions**

At the same time, be aware that freedom to engage in online social media activity is recognized by the National Labor Relations Board (NLRB). If, for example, one of your employees is upset with his or her compensation, and decides to post a complaint on a social network site, the posted statements may be protected by the National Labor Relations Act (NLRA) and firing or disciplining employees based on such posts may be an unfair labor practice. Recently, the NLRB decided that the NLRA protects the right of employees to post statements on social media sites about wages, benefits or working conditions in collective undertaking. The NLRB cites this excerpt of section 7 from the NLRA: "Employees shall have the right to ……engage in other concerted activities for the purpose of collective bargaining ***or*** other mutual aid or protection . . ."

*(Continued on page 11)*

## Is Your Practice Protected Against Bad Behavior By Employees?
## Not always, but make sure you understand some basics to lessen your risk.

*(Continued from page 10)*

**Have a Written Policy**

As discussed with the harassment topic, the most effective tool for employers to defend against liability is to adopt a written policy covering e-mail usage and limiting what employees can post about the practice on social networking sites. The policy must make it clear that employees should have no reasonable expectation of privacy on the practice's computers, email systems and internet connections, and that information exchanged on social networking sites may be accessed by the practice. It should include a statement that in their social networking activities, no employee should post any comment or infor-

*(Continued on page 12)*

## Is Your Practice Protected Against Bad Behavior By Employees? Not always, but make sure you understand some basics to lessen your risk.

*(Continued from page 11)*

mation on behalf of the practice without authorization; similarly, there should be no disclosure of confidential or proprietary information of any kind (including information about patients) without the written consent of the practice. Explain to your employees that online communications (even outside the workplace) that pertain to coworkers and the practice must be appropriate, should not damage the practice's reputation or business interests, or expose the practice to a potential liability. Some businesses have also taken to developing a written "social media contract" stating that violation is grounds for disciplinary action or termination. The policy should cover everything relating to practice computer use, practice-provided cell phone use, and the use of practice logos, trademarks or other intellectual property. Here are additional guidelines on some of the types of activity or content your policy should restrict or prohibit:

- Using practice confidential or proprietary information without authorization.
- Making derogatory, discriminatory, threatening or sexually-related comments towards other employees, toward patients, or toward anyone else associated with the practice.
- Describing or endorsing practice services, equipment, devices, etc. without the practice's consent and a disclosure of the employment relationship.
- Engaging in illegal activities using practice computers, software, etc.
- Accessing personal or inappropriate websites while at work.
- Posting copyrighted information on the practice's website.
- Posting a recommendation or informal review of a subordinate.

**Summary**

Do not wait until an employee complains of harassing conduct or one of your staff members decides to post untrue information about the practice on a Twitter feed to set a policy and procedure for such activities in the practice. These are very serious topics with a potentially large price tag for liability. If you do not have a harassment policy or an electronic communications policy in place or if it has been a while since you have looked at them, seek help from experienced legal advisors to assist you with drafting or revising.■

# Practice Sales: Feedback from the Trenches

By: Daniel M. Bernick, JD, MBA

In previous issues of Issues and Updates, HCG has noted the "uptick" in practice sale transactions over the past couple of years. These deals are continuing to occur. This article discusses some of the more interesting and/or common issues that we have encountered, as legal counsel and business advisors for buyers or sellers, in recent sale transactions.

**Triggers for Sale**

The biggest trigger appears to be demographics. Simply put, there are a lot of baby boomer doctors out there who are looking to exit from practice sometime in the next 6 months to 5 years. All of these are potential candidates for sale.

But age isn't the only deal trigger. In one recent deal, a hospital wanted to set up a special women's care unit, and for that pur-

*(Continued on page 13)*

# Practice Sales: Feedback from the Trenches

*(Continued from page 12)*

pose acquired the mammography business of a nearby physician practice. The physicians are still independent, but they have "de-equitized" their interest in their old mammography business.

In another practice, an ophthalmologist wanted to pare back his practice, in terms of geographic reach, and relations weren't the best with his entrepreneurial associate. The solution? Selling off one of his office locations to the young associate who worked at that location. The older doctor is still in practice, doing well, but has simplified his life and recouped his investment in the sold satellite.

In another practice, the ophthalmologist sold his practice to a private equity firm. The private equity firm didn't really want the medical practice, but it bought it as part of a package deal for the real target, which was the ophthalmologist's licensed ambulatory surgery center.

"De-equitizing" is the central theme of a number of pre-retirement physicians who aren't quite ready to retire, but want to sell their equity now, while they can. The deal is structured with a 3-5 year employment agreement for seller, so that he can continue to work after the sale as a pure employee, at reduced pay. When the time for full retirement comes, the doctor has "pre-sold" his practice.

De-equitizing is also the core concept in various "private equity" deals. These deals are similar to the physician practice management company deals of the 1990s. The owner doctors, fearing a downturn in reimbursement, or other negative future trends, sell their equity to a group of private investors. The owner doctors agree to take a cut in pay, post-sale. This creates additional cash flow for the new investors, inducing the investors to pay big dollars to the doctors to relinquish their equity.

**Valuation Issues**

This is not a new issue, but it is a big, recurring one. There continues to be a huge range in the values paid for small medical practices, ranging from less than $50,000 to hundreds of thousands or several million dollars.

As always, the key variables are specialty, geographics, and profitability. Specialty is a factor because if there is high demand for new recruits, young doctors can attain a high salary income without having to buy an existing practice. And if they are not in the market for purchase of a practice, then potential sellers cannot sell their practices or must cut their asking prices.

Geographics are a factor because more desirable areas (major metro areas, the coasts) are generally more competitive, in terms of doctors seeking patients. This increased competition may enhance the value of existing practices in that area. In other words, it may be easier for a new entrant to acquire a patient base by buying an existing practice, rather than trying to start one from scratch. The heightened demand for existing practices translates into higher prices paid to owners of those practices.

Profitability is a factor because….well, people like money, and profitable practices seem to know how to generate it (money).

Specialty practices have an additional problem. If the local hospital has bought up the area primary care providers, the hospital then controls specialty referrals by these PCPs. Using this leverage, the hospital can force independent specialists to sell at low prices, with the threat that if they do not sell, the hospital will redirect all the specialty referrals to the hospital's own employed doctors.

*(Continued on page 14)*

# Practice Sales: Feedback from the Trenches

*(Continued from page 13)*

Pricing is complicated in private equity deals. A very large purchase price can be justified if the doctor agrees to work for reduced pay after the sale. The doctor is trading future income (compensation) for current capital gains (sale price), which raises the question whether the doctor is getting anything for his practice at all.

**Tax Issues**

The big issue here is with solo PCs that are "C" corporations rather than "S" corporations. Substantial tax can be saved by seller if he successfully claims that the goodwill/intangibles being acquired by buyer are for the doctor's "personal" goodwill, rather than the PC's "institutional" or corporate goodwill. "Successfully" is the key word here. The IRS is well aware of this gambit, and has become increasingly aggressive in challenging such claims, with potentially huge back taxes owed by seller, and penalties. Talk with your tax advisor, and proceed with caution.

**Credentialing Issues**

The typical purchase/sale transaction is accomplished as an "asset sale" rather than a "stock sale." That means that the buyer doctor will need to re-credential himself so that, as of the date of sale, he is associated with the new buyer corporation, rather than seller's old corporation. And credentialing isn't easy. Buyer generally wants extra time to get the credentialing in order before the sale occurs, but seller may not be amenable to a "moving target" (closing date).

**Operation Issues**

These can be big issues if seller doctor is continuing as an employee of buyer's corporation, after sale. Buyer may have big ideas for change, once he has completed the purchase. But seller, as a post-sale employee, usually wants to practice in the exact same way that he always has, for the past 30 years. For example, in a recent transaction, buyer wanted to install EMR in the target practice, after sale, so that there would be a uniform system across all of buyer's locations. But seller MD was "old school" and wanted to continue handwriting his charts. Various workarounds were considered, but all had costs. So the question quickly became the unpleasant one of deciding who was going to pay for this transition cost (buyer or seller).

**Legal Problems**

Sellers who have tax liens or are close to bankruptcy have special problems that make it harder to accomplish a sale or that increase transaction costs (legal and accounting fees). For example, consider a seller in financial distress, who agrees to sell for a discounted price, to get some cash in hand. Buyer may be happy to acquire the practice for a low price, but the victory may be short lived if seller thereafter declares bankruptcy. The purchase of assets by buyer may be questioned or set aside by the bankruptcy court, on the grounds that the sale did not occur for true fair market value.

**Other Assets**

The purchase of the medical practice may be only one of several assets "in play." The purchase of the building in which seller's practice is located may be an important ancillary transaction. Likewise the purchase of an associated ambulatory surgery center. Typically seller wants to unload all of these assets at the same time, so if a problem develops with one transaction, the other transactions may fall through as well.■

**THE HEALTH CARE GROUP**
**140 W. Germantown Pike, Suite 200**
**Plymouth Meeting, PA 19462-1421**
**(610) 828-3888 * Fax (610) 828-3658**
**E-mail: services@healthcaregroup.com**
**Visit our website: www.healthcaregroup**

# IS YOUR HIPAA MANUAL UP TO DATE?

## If Not, Order Your Copy Today

The Office for Civil Rights (OCR) is preparing to conduct Phase Two audits of physician practices and other providers (as well as their business associates) beginning in 2016. Approximately 350 covered entities as well as 50 business associates will be audited to determine their levels of compliance with the Privacy Rule, Security Rule, and Breach Notification Rule, as amended by the Final Rule released in early 2013. While the audits are intended to be educational, any identified HIPAA incidents could result in referral to the OCR Regional Office responsible for your practice which could lead to investigation and substantial penalties. So, what should your practice do to prepare? Consider the following:

Has your HIPAA Compliance Plan been updated since the release of the Final Rule? What about your business associate agreements and notice of privacy practices? Have you conducted a practice-wide risk assessment to determine your practice's security vulnerabilities? Do you have policies and procedures in place to ensure the proper use and disposal of mobile devices? Are you assessing HIPAA incidents properly, using the Final Rule's updated threshold, to determine whether you have experienced a breach and, therefore, must notify the affected individual, the government, and maybe even the media?

If you have questions about the status of your HIPAA Compliance Plan, The Health Care Group, Inc. can help. Visit us at: http://www.healthcaregroup.com/complete-hipaa-complaince-plan-and-guide-details.html or call 800-473-0032 extension 3350 (Cheryl Sprows) or 3316 (Jennifer Cohen).