July 2013

p.s.

SCRIPTS

Legal updates for the health care community from Poyner Spruill LLP

Poyner Spruill LLP
ATTORNEYS AT LAW

WWW.POYNERSPRUILL.COM

INSIDE THIS ISSUE

p.s. If you would like to receive future issues of *Scripts* by email, sign up on our website, www.poynerspruill.com and click on sign up for alerts at the top of the page.

America's Aging Health Care Workforce Presents Major Challenges for Health Care Employers

By Susie Gibbons

The U.S. Census predicts that by 2016, 33% of the country's workforce will be over 50. The impact of the "graying" of American workers is especially significant in the health care industry. The Department of Labor funded a special report on this issue, which can be accessed here. Its recent report includes some startling statistics and projections.

- By 2020, nearly half of all registered nurses will reach traditional retirement age. Currently the average age of a nurse in the United States is 50.
- Nearly 25% of all physicians in a 2007 national survey were 60 or older.
- In 2001, more than 80% of all dentists in the country were older than 45, and the number of dentists expected to enter the field by 2020 will not be sufficient to replace those likely to retire.
- By 2030, the country will need an extra 3.5 million formal health care providers just to maintain the existing ratio of providers to the total population.

The report summarizes strategies that health care providers can use to retain older health care workers, including the following:

- Implementing ergonomic improvements to make job tasks easier for older workers.
- Permitting flexible work hours rather than the rigid shifts typical of most health care jobs.
- Creating a team-based work structure to allow older workers to transfer their institutional knowledge to younger workers and share tasks that may be more difficult for older workers to perform.
- Allowing workers who are 65 or older to work part-time while drawing on their pensions.
- Allowing employees to work for three, six or nine months, and then take a three-month break.

The report is a wake-up call for all health care providers to assess their own workforce and determine whether specific strategies should be implemented to encourage older workers to remain employed.

Susie Gibbons practices in the areas of employment compliance law, employment defense in litigation and administrative proceedings, and ERISA litigation. She may be reached at sgibbons@poynerspruill.com or 919.783.2813.

Using Covenants Not to Compete in the Health Care Industry
Part 1 – Understand the Basics

By Lee Spinks

Covenants not to compete, and their "sister" covenants not to hire or solicit employees, and not to use or disclose trade secrets, are important protections that hospitals, medical practices, and other health care providers should always consider including in their agreements with key employees. Although in some circumstances such covenants might not be enforceable, those circumstances are relatively uncommon, and these covenants can protect a health care entity from serious economic damages resulting from immediate competition by former employees. The basic rules governing these covenants seem simple, but courts examine them closely because they are restraints on trade and competition. To understand the use of covenants for any particular employer-employee situation, first it is important to understand the basic rules themselves.

p.s.

"These covenants can protect a health care entity from serious economic damages resulting from immediate competition by former employees."

1. The covenant must be in writing and signed by the person to be bound. This seems obvious, but too often an employer will include such covenants as part of unsigned policies and procedures and not as part of written employment agreements signed by the employee. To be enforceable, a covenant not to compete must be in writing and be signed by the employee.

2. The covenant must be supported by valuable consideration. In North Carolina, if a covenant is a condition of the initial employment (if the employee is advised that signing a covenant not to compete is a condition of employment), then the employment itself is the valuable consideration for the covenant. The problem arises when an employer wants to start using covenants not to compete with existing key employees. For such covenants to be enforceable, new consideration must be offered to the employee in exchange for the employee's agreement to the covenant. The new consideration can be a promotion – but it must be a bona fide promotion, with true additional responsibilities and true additional potential for increased income. It can be a raise, but not a raise offered to all employees, including those who are not signing covenants. It can be a one-time payment – that payment must be material, something of real value For example, if a doctor makes $500,000 a year, offering $1,000 as consideration for signing an amendment to his employment contract to add a covenant not to compete might be viewed as inadequate consideration. Unfortunately, there is no bright line defining what constitutes adequate consideration, and in each case, the particular facts involving that employee and employer are critical in determining the new consideration to offer.

3. The scope of the covenant must be limited so that it protects a legitimate business interest of the employer. This rule is a bit more complicated. There are two primary considerations – the business activities of the employer while the employee is employed, and the involvement of the employee in those business activities. For example, a hospital system would have a legitimate business interest in protecting against competition by former physician employees only in the practice areas and specialties offered by the hospital. If the hospital did not offer in-patient psychiatric services, then there would be serious doubt that the hospital could enforce a covenant to prevent a former employee from being employed by a different hospital system for the purpose of offering in-patient psychiatric services.

But the rule goes further than merely looking at the services offered by the employer. To be enforceable, the covenant cannot restrict an ex-employee from engaging in activities that he was not involved in (or substantially exposed to) during the term of employment. Consider the employee hired for hospital management with responsibility over that hospital system's owned or managed medical practices. After four years, that employee leaves to work with a competitor, but in a position primarily involving a different area of hospital management – for example, overseeing applications for governmental grants and funding for clinical trial programs. Can the former employer enjoin the ex-employee from accepting (or continuing in) this somewhat different position with a competitor?

It will depend upon the facts. If the new employer does not permit the ex-employee to be involved in the management, recruitment, or other activities related to that competitor's owned or managed medical practices, does not permit him or her to disclose to the new employer any trade secret information, and otherwise ensures that the ex-employee does not violate the terms of the covenant in his or her new position with the competitor, the covenant may not be enforceable, because the ex-employee is engaged in an activity in which he or she was not involved in the former position. Conversely, if the evidence shows that the ex-employee is assisting the new employer with aspects related to the new employer's medical practices, then the covenant would be enforceable.

Finally, the limitation that a covenant protect legitimate business interests is also applied to prevent covenants from being enforced against employees who, if they became employed by a competitor, would not realistically pose a threat of material damage. Covenants not to compete are likely to be unenforceable against employees who are not key providers of services (such as physicians, physician extenders, and management employees) and who otherwise do not have material involvement with or access to information regarding patients, referral sources, financial information, confidential IT systems, business plans, management activities, or other confidential or trade secret information.

4. The covenant must be reasonable as to time and territory. In the traditional employer-employee setting, and absent extraordinary circumstances, a covenant not to compete should generally not have a duration longer than two years. In addition, the territory in which the covenant applies not only must be limited to the territory in which the employer conducts its business, but also will likely be limited to the territory in which the employee was actually involved in providing services. Imagine a health care employer with locations scattered across North Carolina. If an employee is hired to manage or provide physician services in one specific geographic area for this health care entity, then the covenant can prevent competition within that geographic area. The harder questions arise when the employer wants the territory to include the entire state of North Carolina or all states where the employer has locations. To enforce a covenant broader than the territory in which the employee's day-to-day activities are conducted requires a case-by-case factual determination. For example, if the employee was involved in or materially exposed to information about the employer's business activities, patients, referral sources, or other activities over a statewide or larger region, then the covenant may be enforced in this broader territory. Conversely, if the employee had little actual involvement in the activities of the employer's locations outside of the city or other geographic area in which he or she performed services, a court is unlikely to enforce the covenant to prevent competition outside of that city or geographic region.

5. Enforcement of the covenant must not be against public policy. This final rule is particularly applicable in the health care industry. It has most often been applied when a medical practice attempted to enforce a covenant to prevent a physician from competing in a highly specialized practice area or in an area underserved by physicians. In essence, even if a covenant would be enforceable under all the other rules, it nonetheless will not be enforced if doing so would pose a risk to the public health or safety by denying the residents of a community adequate access to necessary health care professionals. Thus, if a rural community had only two orthopedic surgeons who practiced together and one left to form his own practice, it is highly unlikely that the orthopedic surgeon remaining with the original practice could enforce a covenant not to compete to prevent the other one from opening his own separate practice.

These are the basic rules. In another issue, we will examine techniques for drafting covenants to maximize enforceability and deterring employees from leaving to compete against the employer.

Lee Spinks practices in the areas of health law, commercial litigation, and business law. He may be reached at lspinks@poynerspruill.com or 704.342.5278.

Bring Your Own Device Programs and Health Care: Too Risky to Work?

By Tara Cho

Recent workplace surveys report that as many as 87% of employees use personal electronic devices for work, raising compliance, data loss, and security risks for their employers. As a result, designing a workable "bring-your-own-device" (BYOD) program is probably overdue.

The immediate reaction of a health care organization is to ban the practice rather than risk compliance problems. BYOD is a tricky issue, without question, but it's important to consider the realities of the situation rather than getting tied up in an unrealistic policy: 48% of companies claim they would never authorize employees to use personal devices for work, but 57% acknowledge that employees do it anyway. The wave of mobile devices has already flooded your offices. It's time to figure out what to do about it.

Even if you permit BYOD only in limited circumstances, it's still important to lay the ground rules that will help maximize compliance and minimize risk. We can cover only a few key considerations in this article, but here are some of the major issues:

Information Security and Compliance

HIPAA compliance will be the first concern of any health care organization implementing BYOD, and rightly so. HIPAA is heavy on policy and security requirements, so unless PHI will not be accessed or stored using personal devices, then at least part of that compliance program will need to be revisited. The risk of a reportable security breach also may increase, although that risk is likely already present based on the substantial percentages of employees admitting that they use their own device for work regardless of employer restrictions. Enterprise-managed BYOD may improve the odds by providing malware protection, better access controls, remote wiping, and transmission security.

Social Media

If you enable BYOD, social media use may go up, but temper your zeal to prohibit or monitor that use. In recent years, employers have been repeatedly dinged by the National Labor Relations Board for overly broad social media policies, were found liable for accessing employees' social media communication in unauthorized ways, and scaled back reviews of social network sites due to Fair Credit Reporting Act liability. Employers should revisit their social media policies to make sure they are not already running afoul of this rapidly evolving list of pitfalls. You can read more about any of these issues in publications available on our website.

Employee Privacy

Like it or not, employees have some privacy rights not impacted by your warnings that they have no expectation of privacy when using your equipment. Although you can revise applicable policies for BYOD, your employee owns the device and is clearly entitled to make personal use of it. Similarly, that device essentially tracks their whereabouts 24/7 and reflects all manner of activities, such as websites visited, items purchased, books read, games played, photos taken, apps used, and calls and messages sent and received. Your organization must decide the extent to which it needs to know such information and plan accordingly.

e-Discovery and Departing Employees

Inevitably, if employees store work-related information locally, device retrieval may be necessary in legal discovery or when an employee leaves the company. For litigation, strict protocols providing for immediate preservation before employees modify or delete files are crucial. BYOD will add expense and delay to discovery and to the employee-departure process.

Building an Effective BYOD Program

The first step in building an effective BYOD program is to identify your security framework. At minimum, policies and/or terms of use should require device-level security such as strong passwords, malware protection, encryption, time-outs following inactivity, and remote wiping capabilities. Mobile device management (MDM) provides a more advanced option; most will provide employees with a secure tether to the office to access resources remotely using an application on the device. MDM solutions improve upon device-level security by minimizing the risk of data loss and preserving data integrity and access control with containerized solutions. For the command-and-control set, a virtual-desktop infrastructure (VDI) may hold appeal. With VDI, applications and data are stored centrally, unlike the MDM, where some data and apps live locally on the device. Maintaining secure access credentials and effective user authentication are paramount, but the device itself contains no work-related data to be lost or breached. To determine which approach is best, inventory your business units, their activities, and their use or proposed use of mobile devices.

The next major step is to provide a program framework through documentation. A written program policy is needed to establish privacy boundaries and set security expectations. You also should review existing social media, security, and compliance policies to ensure you have not set contradictory requirements or limitations. The last piece of documentation should be terms of use that employees commit to (including remote wiping of all content) in exchange for the privilege of using BYOD.

Last, support your security and policy framework with training, reminders, and program reviews to help employees remember the requirements and to help your organization establish legal compliance.

Tara Cho's practice focuses on privacy and information security. She may be reached at tcho@poynerspruill.com or 919.783.1079.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW