BLR®
a Simplify *Compliance* brand

Legal and Tax Issues of Telecommuting

SPECIAL REPORT

FEATURES

Allowing multistate telecommuting? Don't forget taxes, unemployment insurance

From: West Virginia Employment Law Letter

When considering adopting a telecommuting policy, employers and HR professionals may carefully and thoughtfully weigh the potential for equipment and facilities cost savings, the ability to recruit and retain employees outside the local market, and an increase in morale and productivity against the sometimes complex logistics of remote work and communication, new challenges of remote management, and the idea that telecommuters may become "out of sight, out of mind" or, worse, unproductive. Yet there are a few legal considerations of remote work—particularly when employees are employed in multiple states—that sometimes slip through the cracks. These details may create unnecessary head-scratching, scrambling, and paperwork—not to mention penalties—later in the employment relationship.

Let's say your corporate office is located in state A, but with the adoption of your telecommuting policy, you now will have employees working out of their homes in state B.

Where do I owe taxes?

Though your business may have no operations in state B beyond the presence of your telecommuting employee, telecommuting work can create tax liability in that state for both you and the employee. At a time when states are hungry for more revenue, many will be eager to collect if they learn you have employees working within their borders.

A 2010 New Jersey court decision first revealed this liability. In the case, a Maryland corporation dutifully withheld and remitted New Jersey income tax from the paycheck of a single employee who had relocated and telecommuted full-time from her home in New Jersey. The tax withholdings alerted the New Jersey Division of Taxation of the arrangement, and the division asked for more. The division and the New Jersey Tax Court held that the employer also owed New Jersey corporate business taxes because of the "nexus" with the state—the nexus being one employee typing away on her laptop. The Superior Court of New Jersey agreed, holding that the employee's full-time work developing software code in New Jersey and both parties' right to New Jersey's legal protections entitled the state to a piece of the pie, despite the employer having no other connection to the state. *Telebright Corporation Inc. v. Director, New Jersey Division of Taxation.*

New Jersey isn't alone in this practice. According to a 2012 BNA survey of state tax departments, 35 other states also would find a "nexus" creating tax liability within their state for employers with telecommuting employees residing there, even when

the employer has no other connection with the state. Only six states—Indiana, Kentucky, Maryland, Mississippi, Oklahoma, and Virginia—clearly stated that this sort of telecommuting arrangement wouldn't give rise to additional tax liability.

Where do I owe unemployment insurance?

When thinking of the beginning of the telecommuting relationship, you must also consider the end. If your telecommuting employees are laid off and choose to draw unemployment, in which state must they file (and which state will turn to you for unemployment insurance contributions)?

As with taxes, unemployment claims generally are filed in the state in which the employee physically performed the work. Most states' unemployment statutes define employment similarly:

> *An individual's entire service, performed within or both within and without this state, if (a) the service is localized within the state (i.e., performed either entirely within the state or performed both within and without the state if the service performed without is incidental to that performed within); or (b) if the service cannot be considered as localized in any state but some of the service is performed in the state and (i) the individual's base of operations, or if there is no base of operations, then the place from which such service is directed or controlled, is in the state.*

In other words, the first factor considered is where an employee's work is localized. Further inquiries occur only when the work can't be pinpointed to any one location. But is a telecommuting employee's work localized in the state of her residence or the state from which the work is directed?

Very little case law and specific legal guidance currently exists on this matter. The most instructive guidance comes from a New York Court of Appeals case in which an employee who worked entirely from her home in Florida was found ineligible for unemployment in New York, where her employer's business was based. The court held that because the employee was physically present in Florida when she worked for her employer, her entire service was localized *in that state* for unemployment compensation purposes.

Therefore, in most cases, unemployment insurance payments for telecommuting workers should be paid to the state from which the employee is actually conducting the work.

Bottom line

These additional areas of uncertainty and potential liability may leave employers reluctant to adopt otherwise workable telecommuting policies for out-of-state workers, but don't forget that even these costs may still be outweighed by the ability to

retain or recruit valuable employees, reduce employee travel time and expenses, and allow employees to work in an environment they find most productive.

Before allowing workers to telecommute, be certain that each employee reports to you the state from which she actually will be performing the work so you can properly evaluate whether your business will take on additional tax and unemployment insurance responsibilities. ■

From the home office: employer considerations for telecommuters

From: Wisconsin Employment Law Letter
By: Danielle E. Baudhuin

> **Telecommuting increased from 19% of the U.S. workforce in 2003 to 24% in 2015, according to the U.S. Bureau of Labor Statistics."**

Working from home has become an increasingly common practice for many employees in a variety of professional settings. Telecommuting increased from 19% of the U.S. workforce in 2003 to 24% in 2015, according to the U.S. Bureau of Labor Statistics (BLS). Employees in management, business, financial operations, and professional occupations worked from home in 2015 at a rate of approximately 36%. Further, research from recent years has shown that more Gen-Xers and Baby Boomers than Millennials prefer to work from home. So, with the recent upswing in telecommuting and the anticipated growth of working from home, what are the legal issues that employers should be on the lookout for?

To permit or not to permit telecommuting

Setting aside the issue of whether telecommuting can ever be a required reasonable accommodation for a disability, permitting employees to telecommute can create significant employment concerns. For example, it's more difficult to monitor employees who are working from home. As a result, nonexempt employees who telecommute can more easily create overtime obligations for your company.

Moreover, if you allow some employees, but not others, to work at home, you may face disparate treatment discrimination claims. And injuries to employees who are working from home with your consent can raise interesting worker's compensation questions.

So, your first consideration should be whether to permit telecommuting. If the answer is yes, then you should take appropriate actions to minimize the risks of liability.

Unpaid overtime

Remote work performed by employees often results in overtime liability for employers. You should carefully monitor your nonexempt employees' telecommuting time. Employees should be required to notify a supervisor or clock in electronically when they begin their workday and notify a supervisor or clock out at

the conclusion of their workday. Employees should also be required to keep track during the workday of all breaks longer than 30 minutes, including lunch breaks. If you have an overtime policy that requires a supervisor or manager to preapprove overtime, you should inform your telecommuting employees that the rule applies when they work from home.

Another form of working from home is compensable work performed by an employee before the start of her workday or after she has completed her workday (often referred to as "off-the-clock" work). In our electronic world, employees may read and respond to work e-mails, including messages from supervisors, clients, or customers, while they're technically off the clock. Similarly, employees may make or receive business-related telephone calls during their off hours.

Assuming off-the-clock work isn't *de minimis* (insignificant or performed infrequently), it may be compensable. And if it results in the employee working more than 40 hours in a workweek, you must pay her time and a half for her off-the-clock hours.

You should have a written policy that prohibits off-the-clock work, including reading and responding to work-related e-mails and telephone calls without approval. When you become aware that an employee has violated the rule, you should enforce it with counseling or, if necessary, discipline. You don't want to be in a position where you're aware that your nonexempt employees are working off the clock and tacitly accepting such work without paying them.

Privacy and confidentiality: cell phones

Many employees have work e-mail accounts linked to their phones, which is one of the most basic, and arguably the most widespread, form of telecommuting. However, this simple practice might open your company to hacking or data breaches if employees are lax with the security of their phones.

First, a simple privacy concern involves the accessibility of employees' cell phones. If an employee leaves his phone unattended or his phone is stolen, third parties may gain access to your corporate or client information. You should impose certain restrictions and policies to ensure that your employees take care to guard the information on their phones:

- Require a password to access the content of phones.
- Turn off "previews" of incoming e-mails or texts on the phone. That limits what someone can view even when the phone is password-protected.
- Enable remote resetting or "wiping" of data if a phone is lost or stolen.

Second, educate employees on possible hacking threats. For example, public charging ports at airports or coffee shops can be an unsuspecting host for viruses that can either damage information on a cell phone or steal the user's data,

including private and otherwise secure information. Many people don't consider the security risks when they connect to a public charging port because they're either unaware of the danger or don't suspect a threat. A recent experiment found that more than 80% of people who used a public charging port at a conference didn't ask about the port's security before connecting their phones. Simply educating your employees could substantially limit the risks of a data breach.

> "As with cell phones, you should take care to educate employees on the security risks of unsecured Internet access and impose strict policies for the security of company information."

Privacy and confidentiality: Wi-Fi

Working remotely can also create risks for employees who use otherwise secured computers. Public or unsecured Wi-Fi hotspots open computer users up to a substantial risk of both their personal and corporate information being hacked. Hackers can intercept information that a user sends from a computer over her employer's network. That means the hacker sees and receives all of her information, including passwords, user names, and other information, which can allow him access to even more restricted or confidential information.

As with cell phones, you should take care to educate employees on the security risks of unsecured Internet access and impose strict policies for the security of company information, including:

- Prohibit employees from telecommuting while they're connected to unprotected or public Wi-Fi.
- Offer virtual private network (VPN) software to secure connections and protect information.
- Provide cellular hotspots for employees using their computers remotely. Although the additional cellular data use may impose a higher cost for your company, a secured cellular hotspot offers a password-protected connection for employees anywhere with cellular reception.

Worker's comp claims

Working remotely also raises some interesting worker's comp concerns for employers. Under Wisconsin worker's comp law, an employer is liable when an employee sustains an injury in the course of performing services "growing out of and incidental to his or her employment."If one of your employees is injured while he's working remotely, you could be held liable under that provision.

What if an employee is supposed to be working remotely but is injured while he's performing some task unrelated to his job? How can you be certain that the employee was actually performing services incidental to his position when he was injured?

You can limit possible fraudulent or unsubstantiated worker's comp claims by creating a telecommuting policy that addresses which employees are permitted

to work remotely, when they may work remotely, and where they are permitted to work remotely. For example:

- Require prior authorization before an employee may work remotely. That way, you can restrict telecommuting to employees who you believe can work without much supervision.
- Require that any employees who work remotely have a designated remote office or desk, and provide training and information about work-station setup and ergonomics.
- Require strict time reporting, even for salaried employees. That way, you have a record of when the employee is working or taking a break, which may help if a telecommuting employee is injured remotely and there's a dispute over whether the injury took place during working time or a break.

Bottom line

Telecommuting or working remotely can have several benefits for both employees and employers. Employees may appreciate the freedom to work around their busy schedules, and employers may benefit from happier employees, which will result in lower employee turnover. However, as we've noted in this article, the benefits of telecommuting come with certain risks.

If you permit your employees to work remotely, you should create and implement policies that explain your rules and expectations of telecommuters. Education and communication can help you stave off possible future legal concerns. ■

Telecommuting GPS: mapping out the detours of working remotely

From: North Dakota Employment Law Letter
By: Jo Ellen Whitney, Davis Brown Law Firm

Everybody loves telecommuting and has nothing but great things to say about it. According to many articles you read these days, it's clearly every employee's dream. But is telecommuting really the key to happiness for employees and employers? Maybe.

An arrangement with many different names

HR pundits will tell you that Millennials "demand" telecommuting. That's supported by a 2017 Global Workplace Analytics study that showed a 115 percent increase in working from home over the last decade, with approximately three percent of the U.S. workforce currently working from home. However, other sources, including the U.S. Department of Labor (DOL), note that there has been a significant decrease in

telecommuting over the last two years, with large corporations such as Yahoo, Bank of America, Aetna, and IBM canceling their telecommuting programs.

So what gives? Is telecommuting a panacea that will solve all of your workplace problems, or is it a drag on productivity and teamwork? Like so many things in HR, the answer depends on what you're really talking about.

Part of the disconnect is that when we talk about the various forms of telecommuting, we aren't necessarily comparing apples to apples. It's more like comparing apples to dragon fruit. Telecommuting comes in a many forms, and employers must carefully plan for the type of telecommuting arrangement they want to allow—and what they won't allow. In fact, "telecommuting" might not even be the appropriate term for what happens at your company. You might use terms like "flexible scheduling" or "working remotely" to describe the arrangement you've set up with your employees. And "working from home" describes a specific type of telecommuting where employees work from a home office on a regular schedule, possibly reporting back to the "main office" periodically.

Employees work from coffee shops, answer e-mails on their cell phones as they travel, send texts to customers, and engage in countless other activities away from the main office during 'nonworking' time."

Almost every employer allows some type of ad hoc telecommuting, formally or informally. Employees work from coffee shops, answer e-mails on their cell phones as they travel, send texts to customers, and engage in countless other activities away from the main office during "nonworking" time. As a result, you should assess how much remote work your employees are doing and implement policies that address their use of technology and your expectations of them when they aren't working in the office.

Common issues and concerns

Accountability. Employers typically start with questions about accountability, such as how to ensure the quality of a telecommuting employee's work or properly track her hours. Another concern is losing the cross-pollination of ideas. In other words, if an employee isn't in the office, he won't be interacting or brainstorming with the team, and group work will suffer. Cross-training also becomes an issue.

One of the stumbling blocks is the inability to actually measure what a successful job looks like. That can be true whether an employee toils away at the office, works remotely, or establishes a telecommuting office in her home. You should ask questions like:

- What does acceptable performance look like?
- What are the metrics that apply to the position?
- How are those metrics used, and how are they regularly audited or accounted for?

Accountability should be measured on both an individual and a team level for an employee who doesn't work in the office. The loss may be felt more keenly for one type of job than another. As part of your accountability assessment, you should measure how much a team suffers from losing the physical presence of the telecommuting employee.

Wage and hour issues. Another common concern involves wage and hour issues. First, you must ensure that time during which the employee isn't performing work is being properly recorded. In a home office situation, it's very easy for an hourly employee who's "on the clock" to wander away from his desk to make a sandwich, pet the dog, fold some laundry, or engage in myriad other chores to avoid work. Unlike at the workplace, there isn't someone to give him the side eye and tell him to get back to his desk. That's why it's necessary to assess your jobs and have clear metrics for determining which ones can be successfully performed by a telecommuting employee. Decide whether you expect the employee to complete a certain amount of work each day, or set an error rate or some similar way to evaluate whether he is using his time on the clock appropriately.

Another concern arises for hourly employees who engage in ad hoc telecommuting. If your nonexempt IT person consistently gets calls from colleagues while she's on vacation, traveling, or at home, she should be paid for that working time. It can be difficult to get employees to appropriately record for compensation purposes all of their e-mails, text messages, and other responses to issues that arise while they're away from work. Minor things like a quick "I'll be five minutes late" text don't need to be counted as time worked. But you should plan to pay a nonexempt employee if you interrupt her vacation to have a 15-minute conversation about how to resolve a firewall issue. Employers need to have clear expectations that time worked will be fully accounted for and fully paid.

Travel to the office by telecommuting employees may also implicate wage and hour issues. If an employee who normally works from home or from her local coffee shop is required to report to the workplace for a meeting, would her travel time be considered an unpaid commute, or is it paid working time? The answer depends on how you draft your telecommuting policy. If your policy requires telecommuters to show up at the office periodically, such as one day a week or for certain quarterly meetings, you can count travel time as unpaid commuting time for hourly employees. However, you should be aware that if an employee must travel a significant distance to get to the office, his travel time may have to be paid—and could result in overtime.

OSHA and workers' comp. You should address safety and workers' compensation issues *before* an employee sustains an injury while working from home or ad hoc telecommuting. While the Occupational Safety and Health Administration (OSHA)

doesn't typically inspect home worksites, if an employee sustains an injury while he's telecommuting, the injury may still be recordable or reportable.

For example, if a telecommuting employee drops the laptop she uses for work on her foot and ends up in a cast, her broken foot would generally be a recordable OSHA injury as well as a compensable workers' comp injury. If the house burns down because the wiring is bad and the employee dies in the fire, it wouldn't be an OSHA or a workers' comp issue because the fire was related to a defect in the home where the employee lived.

> **When you develop your telecommuting policy, you should check with your insurance company to make sure you have appropriate coverage."**

Employees who work from home or another remote environment should be thoroughly trained on the appropriate process for reporting any injuries that may be work-related. Employers frequently express concern that an employee will injure himself playing softball, waterskiing, or doing something entirely nonwork-related and then claim the injury was sustained while he was performing work at home. Careful policies requiring telecommuters to report any injuries promptly, and closely monitoring all employee injuries can help you alleviate such issues. However, keep in mind that there's no perfect way to ensure that potentially compensable injuries are in fact work-related, whether they happen at a home office or on a remote jobsite.

Third-party visitors and liability. Issues may also arise if a third-party visitor to an employee's home office is injured. For example, you may be liable if a customer who goes to an employee's home to evaluate your company's product trips over the employee's dog and breaks his arm. When you develop your telecommuting policy, you should check with your insurance company to make sure you have appropriate coverage for such incidents.

Data privacy and security. A critical telecommuting issue many employers may not consider is data security. How do you ensure that telecommuters comply with your computer use policy if they access from unsecure places or myriad devices?

It's critical to ensure data privacy and security for both home-based and ad hoc telecommuters. If employees are remotely accessing your internal computer systems or removing data from your premises to work remotely, your privacy and security policies must address when, how, and by whom data may be accessed. Ensure that all information is password-protected and encrypted, and inventory all devices, recording their make and serial number information so you can track stolen or damaged devices. It's advisable to audit the security measures on each device and enable GPS and remote wiping capability, if available, on any devices used for conducting company business.

Your policies should make clear that any equipment employees use to accesses company-based systems may be monitored by the company and remotely wiped if necessary. Employees should understand that they may be required to turn over

their devices for review and evaluation by the company. They should also understand that any improper access or use of data, such as a ransomware attack, must be reported to the appropriate person immediately to prevent other systems and data from being compromised.

You also need to discuss with incidental or ad hoc telecommuters whether the Wi-Fi they use carries an unacceptable risk. Multiple studies have shown that free Wi-Fi ports often contain viruses and other malware. Many employees will click "Yes" on a terms of use agreement, not understanding that they're also allowing the Wi-Fi provider to download software onto the equipment they're using. Free sounds great until it shuts down your system, spams your client list, and compromises your bank account information. In developing any privacy and security policy, don't forget the practical applications. It usually isn't the software that creates the problem—it's the people using it.

Discrimination. Finally, it's important to determine whether your telecommuting policy is fair and applied equally to all employees. Telecommuting can be a source of contention in disability discrimination cases when employees demand to telecommute as a reasonable accommodation under the Americans with Disabilities Act (ADA). If you allow telecommuting and you have telecommuting policies in place, it can be difficult to decline an employee's accommodation request.

Certain jobs lend themselves better to being performed remotely. As an employer, you'll want to carefully assess which jobs will allow employees to work from a remote location either full-time or part-time and which jobs truly require employees to be present on-site. You should do an assessment of essential job functions before you receive a request for accommodation so you can explain to the Equal Employment Opportunity Commission (EEOC), the *North Dakota Department of Labor and Human Rights,* or any other administrative agency looking into a discrimination charge that an employee's request to telecommute was unreasonable.

Creating your company's telecommuting policy

In assessing or creating a telecommuting policy, keep a few key elements in mind:

- Understand how your employees currently work remotely as regular or incidental telecommuters. Seek their input to determine how or if telecommuting is appropriate for your company.
- Make sure your policy addresses your expectations for when employees will be in the office, how they will be available, and how they will maintain the security of your data and equipment.
- Remember that the key to a successful policy is careful planning, employee input, and cooperation as well as follow-up by the employer to ensure accountability. ■