MedPro Group
Berkshire Hathaway's dedicated healthcare liability solution

Can Your Office Benefit From a Portable Device Policy?

MedPro Group Patient Safety & Risk Solutions

More than ever, people are using portable electronic devices (such as laptops, cell phones, tablets, e-readers, and other "smart" devices) as part of everyday life. This trend will no doubt continue to grow as a result of technological advances and consumer demand.

Although these devices can be entertaining and convenient, they also can create challenges in the workplace, including healthcare settings. Let's consider the risk management implications of this "age of instant access" for medical practices.

The Case for Use of Portable Electronic Devices

Charlotte is a working mom who has a toddler in daycare. Typically, she checks in with her daycare provider once a day around 12:30 p.m. These "touch-base" calls generally take only a few minutes of Charlotte's time. Calls like these are common in the workplace and were typical in many work environments before telephones became mobile.

Charlotte isn't taking advantage of her employer; rather, she is attempting to avoid workplace distractions by ensuring that things are going well with her child. Few employers object to this type of communication — whether on a work phone or a personal cell phone.

Compare and Contrast the Issue

The same medical practice that employs Charlotte hires another employee named Diane. Diane has two elementary school-aged children who are watched by a neighbor in the afternoons. Just as Charlotte calls to check in on her toddler at daycare, Diane calls her babysitter in the afternoon to check on her kids. However, Diane is good friends with the babysitter, so these calls are rarely brief.

Typically, Diane multi-tasks while she talks to the babysitter. She walks around the office speaking into her phone's headset. At the same time, she completes various clerical tasks, and sometimes even interacts with patients. She may schedule appointment or collect payments, all while chatting on the phone.

Many times, Diane's conversations with the babysitter include personal information, (e.g., details about arguments with friends or ongoing family issues). Further, Diane texts her husband throughout the day and checks in on her personal social media accounts frequently.

Inconsistency

The medical practice that employs Charlotte and Diane does not have a staff policy about portable electronic devices, personal calls, or personal use of social media. Without these policies in place, it might be difficult to ask Diane to alter her phone habits. After all, Diane continues to work while she's on the phone — Charlotte doesn't.

If Charlotte has always been allowed to make personal phone calls to her daycare provider, then isn't Diane being discriminated against if she is forbidden to call her children's babysitter?

The accommodation of allowing employees such as Charlotte to make a reasonable number of personal phone calls during work hours shouldn't be misinterpreted if another employee puts a different spin on the matter.

Additional Risks

Multi-tasking and multiple distractions can increase the risk of errors. In any healthcare environment, errors may pose harm to patients. Errors may range from noting a patient's appointment for the wrong day or time (an inconvenience) to misfiling a biopsy report (a potentially significant injury). Distractions caused by multi-tasking can also antagonize patients who, although unharmed, may perceive these interruptions as disrespectful or dangerous.

Expanding on the issue of security, violations of personal privacy can occur if conversations are overheard — not just by individuals in the office, but by persons who are on the other end of a telephone conversation. Further, if telephone conversations can occur anywhere within the office, inadvertent eavesdropping may increase.

The use of portable electronic devices in the workplace may also tempt employees to engage in inappropriate activities. Reports of cyber security breaches proliferate on a nearly daily basis.

Hospitals and other healthcare organizations have reported significant security breaches as a result of: (a) employees who use their cell phones to take pictures of patients' social security numbers and credit cards; (b) illegal transmission of electronic patient files via mobile devices; and (c) numerous other types of criminal activity.

Policy Planning

Every medical practice should be committed to providing safe, courteous, and efficient patient care. As part of this effort, practices should consider implementing an employee policy related to the use of portable electronic devices.

The policy should note that, to the extent possible, personal phone calls should be taken care of during breaks or lunchtime. The policy should be broad to cover a variety of situations and to keep it as fair as possible. In Diane's case, there is no reason why

she can't call her children's babysitter during her afternoon break, and Charlotte can touch base with her daycare provider during her lunch break.

On occasions when an employee is forced to make or receive personal calls outside of personal time (e.g., the daycare provider calls to report that Charlotte's toddler has a fever, or the school calls because one of Diane's children was hurt on the playground), then these infrequent calls can be promptly managed — or, if they are not emergencies, can be deferred until a more appropriate time.

In addition, the presumption that friends or family can chitchat with an employee at work should be addressed, courteously but firmly.

Employees should not be allowed to carry personal portable devices with them throughout the office. Rather, the devices should be turned off during business hours and kept in employees' purses, bags, or desks. They can check and respond to personal calls during their break time.

Also, the practice's portable device policy should prohibit the photographic use of phones in the office; abuse of this policy might be cause for immediate termination of employment.

Finally, employees should be educated about the medical practice's portable device policy — and the consequences of violating the policy — as part of new staff orientation and periodic staff training.

Conclusion

Every technological advance entails potential new opportunities, e.g., expanded services and enhanced income. At the same time, new technologies may pose challenges that won't be identified unless risk assessment is part of the ongoing function of the medical practice.

As part of an ongoing commitment to patient privacy and security, most medical practices already have in place policies and procedures that address security of computers, use of passwords, message encryption, and so on.

The next step in security is making sure that employees understand the role — and necessary limitations — associated with the use of portable electronic equipment in the scope of medical practice. For further information about cyber security, healthcare providers and practice administrators are urged to contact their MedPro Group patient safety and risk consultants or their personal attorneys.

The information provided in this document should not be construed as medical or legal advice. Because the facts applicable to your situation may vary, or the regulations applicable in your jurisdiction may be different, please contact your attorney or other professional advisors if you have any questions related to your legal or medical obligations or rights, state or federal statutes, contract interpretation, or legal questions.

The Medical Protective Company and Princeton Insurance Company patient safety and risk consultants provide risk management services on behalf of MedPro Group members, including The Medical Protective Company, Princeton Insurance Company, and MedPro RRG Risk Retention Group.

© MedPro Group.® All Rights Reserved.