MedPro Group
a Berkshire Hathaway company

Can Your Healthcare Practice Benefit From a Personal Electronic Device Policy?

Patient Safety & Risk Solutions

PEACE OF MIND | EXPERTISE | CHOICE | THE MEDPRO GROUP DIFFERENCE

More than ever, people are using personal electronic devices (PEDs) — such as laptops, cellphones, tablets, e-readers, and other "smart" devices — as part of everyday life. This trend will undoubtedly 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. Although seemingly harmless, employee use of PEDs can have both risk management and patient safety implications.

A Double-Edged Sword

PEDs offer many benefits when used responsibly, but inappropriate use can result in a range of outcomes, from minor irritation to serious problems. Consider the following example of two healthcare practice employees who both use PEDs during working hours:

> 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 cellphone.

> The same healthcare practice that employs Charlotte also employs Diane. Diane has two elementary school-aged children who are watched by a neighbor in the afternoons. Just as Charlotte calls to check on her toddler, 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 appointments 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.

The healthcare practice that employs Charlotte and Diane does not have a staff policy about PEDs, personal calls, or personal use of social media. Without a policy 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 bottom line is that 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.

Risk and Safety Concerns

Multi-tasking and multiple distractions can increase the risk of errors. In any healthcare environment, errors may pose harm to patients. In the example of Diane, errors might range from noting a patient's appointment for the wrong day or time (an inconvenience) to misfiling a biopsy report (which could lead to a potentially significant injury). Distractions caused by multi-tasking also can 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 PEDs in the workplace may also tempt employees to engage in inappropriate activities. Reports of cybersecurity and HIPAA breaches proliferate on a nearly daily basis, and healthcare organizations have reported significant security issues as a result of employees using cellphones to take inappropriate pictures of patients or patient information (e.g., health information, credit card numbers, social security numbers), illegally transmitting health records, and other types of criminal activity.

Policy Planning

Every healthcare 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 PEDs.

The policy should note that, to the extent possible, personal phone calls should be taken care of during breaks or lunchtime. Additionally, the policy should be broad to cover a variety of situations and to be 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.

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 make small talk with an employee while he/she is working should be addressed, courteously but firmly.

Practice policy should prohibit employees from carrying PEDs 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 breaks.

Also, the practice's PED policy should prohibit the photographic use of phones in the office, which could potentially lead to security and HIPAA breaches; abuse of this policy might be cause for immediate termination of employment.

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

Take-Away Message

Every technological advance offers potential new opportunities, e.g., expanded services and convenience. At the same time, new technologies might pose challenges that won't be identified unless risk assessment is part of the ongoing function of the healthcare practice.

As part of an ongoing commitment to patient privacy and security, most 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 PEDs in the healthcare setting. For further information about cybersecurity, healthcare providers and practice administrators are urged to contact their MedPro Group patient safety and risk consultants or their personal attorneys.