What should be part of your computer-use policy?

As computer use proliferates, people use computers for many purposes both acceptable and not-so-acceptable. In a business context, the clash of uses frames controversies over computer-use policies, pitting privacy of employee communications against employer efforts to manage and control digital information assets.

Managers and employers are concerned about these issues because the controversies create emotional reactions over possible perceptions of privacy invasion. A good place to start drafting a working policy document is on the SANS Institute's web site. The Institute specializes in training computer security specialists and in maintaining current awareness resources on information security issues. It has an Information Security Acceptable Use Policy form that it encourages all users to download and adapt to their particular situations available at http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf.

While you are drafting your computer-use policy, it is prudent to include the seven key elements of an effective policy that the U.S. General Accounting Office concluded were important after an analysis reported in Employee Privacy-Computer-Use Monitoring Practices and Policies of Selected Companies (GAO-02-717 (September 2002) available online at http://www.gao.gov). They include:

1) a reminder that hardware, software, and data are proprietary assets;

2) a reminder that there is no expectation of privacy on business computer systems;

3) a comprehensive definition of improper uses;

4) a discussion or definition of acceptable or allowable uses;

5) a policy on protecting confidential or sensitive information;

6) a list of disciplinary actions for violators of the policy; and

7) an employee acknowledgment of the policy and the employee's agreement to abide by the policy.

Proprietary assets: This element refers to the concept that the hardware, software, and data in your computer system are business assets and that they are owned by the practice or business. It is prudent to emphasize that data created, accessed, or stored in the system (a business asset) are, themselves, business assets. As business assets, they are subject to monitoring, audit, and review.

No expectation of privacy: This element reminds users that they are not to assume that communications on the business computer system will be private. Electronic mail, photos, and other data downloaded for business (or fun) will be subject to audit and review.

Definition of improper uses: This element includes a ban on offensive material, including obscenity, sexual content, racial, religious, and sexual-orientation slurs, insults to personal characteristics, and harassment. Here, an opportunity for controversy arises because the nature of practice may include references to words and matters that would ordinarily might be improper. If your business or practice handles cases concerning allegations of obstetrics/gynecology malpractice or prosecution or defense of rape, you might consider special rules to deal with that material. In addition, if you use software to monitor and filter your system for offensive material, you risk excluding the words and concepts that are most relevant to your practice areas.

Definition of allowable uses: This element includes what employees are allowed to do on the system, including what personal uses you will allow. Here is where you crack down on the senior partners child (or other relative or the senior partner him- or herself) who wants to load and play a fresh new game that (you do not know) was just downloaded from one of the underground sites on the Internet. The game may install viruses, Trojan Horse programs that are hidden and that corrupt your files, and back-door programs that allow access to your system from anywhere in the world by underground characters.

Protection of sensitive or confidential information: This is required by ethical rules and by recent statutes dealing with personally identifiable information. It includes names, addresses, telephone numbers, credit-card data, medical data, and all other confidential matters that lawyers maintain. This is a potential problem area for attorneys if they do not understand just how public transactions are in the electronic world we are creating. The casual assumption of privacy in the use of electronic tools may lead to ethical lapses arising out of compromised information.

Disciplinary action for violations: This element puts some teeth into the policy and assures attention to it.

Employee acknowledgment of policy: This element generally includes a signature on a statement of the policy that it was read, understood, and the employee agrees to it. That document is generally supplemented by a log-in screen that contains a statement of agreement with the computer-use policy that the user clicks on to indicate assent or access will be denied.

These seven elements help you and your employees maintain an effective computing relationship.