
Office Internet Usage Policy – Should I have one?

If you read last month's article you know I was going to review a new tablet PC from Toshiba this month. However, since I have not been able to pry it out of my network specialist's hands long enough to take a look at it, I am going to have to write on another topic. One of the areas that I very rarely see addressed is acceptable Internet usage. Almost every physician office, even in the most remote geographical locations in the United States, has some form of Internet connectivity. There are definite advantages to having high speed Internet access for issues like eligibility verification, electronic claim filing, e-filing prescriptions, and researching and printing patient instructions. Some of the critical applications in the office such as certain EMR programs, scheduling, and billing services can be hosted offsite and available only via the Internet. What is not addressed, either verbally or in writing, is what is and is not acceptable when using the Internet; whether that means email, instant messaging, browsing web pages, or playing music. The only time I see this issue come up is in a reactive mode, but most of the more common problems could be averted if everyone knew the practice guidelines for acceptable Internet behavior.

The biggest reason for implementing a policy is, of course, HIPAA and its guidelines for privacy and security regarding patient information, but there are other liability issues to consider. Emails have been considered legal documents for the last seven years or so and also can easily be intercepted as the majority of emails have no encryption. Instant messaging via an outside provider, such as Yahoo, MSN, or AOL, can be used by spyware to infiltrate your internal network. And while the above threats are probably some of the most serious, but less likely, you probably would not want to take a chance regarding HIPAA violations, lawsuits, or the possibility of exposing confidential internal information.

Next to legality, the second biggest impact of Internet misuse is financial; it costs your practice money either to have an IT specialist remove spyware, or in lost employee productivity due to web surfing or eBaying. Some examples of Internet misuse we have been asked to address are: downloading screensavers and/or music – these almost always contain some form of spyware that can send data back to an anonymous website; overuse for non-business purposes – employees spending more time 'surfing the Web' than on job related tasks; pornography – employees accessing porn sites during and/or after business hours; posting of resumes – looking for a new job using the resources of their current job; or even running second businesses via the Internet from the office computers.

To address these issues, I recommend implementing two things: a written policy that each employee signs to acknowledge and an Internet filter (either software or hardware). Most Internet filters are transparent to the end user, however be sure to get one that is flexible enough to add and remove criteria if necessary. As always, if you would like more information regarding Internet usage please contact Carin Slader, 864-297-8889 or cslader@mdserv.com