

Anti-Virus Policies and Procedures

(AAP recommended policy modified by PCC)

Anti-Virus Policy:

Our practice is committed to taking the necessary steps to prevent computer viruses from infecting the practices computer system. Practice employees must adhere to the policies and procedures listed below:

Employees must not use Microsoft Outlook to read email messages.

Employees must not use Microsoft Internet Explorer to access the Internet.

Personal computers used in the office should be installed behind the practice's firewall.

Employees should not open email attachments if he/she is not expecting an attachment from someone he/she knows or trusts.

Employees are strictly prohibited from using illegal or "pirated" software on the practices computers.

Employees must scan files attached to email messages, files downloaded from the Internet, and files on diskettes brought from home with anti-virus software prior to opening them in practices computer system.

Employees are prohibited from utilizing diskettes on the practices computer system if they suspect its files are infected with a virus.

Anti-Virus Procedures (for Microsoft Windows PCs):

Employees must scan files attached to email messages, files downloaded from the Internet, and files on diskettes brought from home using the practices virus scanning software prior to being opened on the computer. The virus scanning software may automatically scan for viruses when files are being downloaded onto the practices computer system. If they are not, the employee must manually start the program.

The System Administrator or Security Official must conduct a virus scan of the practices computer network server and workstations at least once a week. Employees should be instructed to log off, but not shut down their workstations once a week so the anti-virus software program can run in the evening.

When the practice purchases new computer software, the System Administrator or Security Official must make sure it is shrink-wrapped and must check the diskettes prior to installing the software on the computer system.

The System Administrator or Security Official must make sure that diskettes used to store computer software programs are write-protected or protected against information from being saved on this disk. This prevents viruses from being copied onto diskettes containing important information.

If the practice obtains new computer equipment, but the "new" computer is in reality a recycled one that someone else used before, the System Administrator, Security Official, or information technology consultant installing the computer should conduct a "low-level format" of the hard drive. This will destroy any viruses that may be on the hard drive as well as get rid of illegal copies of software.

If the practice obtains a recycled computer that comes pre-loaded with software or if the hard drive is pre-formatted, the System Administrator, Security Official, or information technology consultant should scan the hard drive for viruses before the practice starts using the computer.

All software should be acquired from reputable dealers.

Anti-Virus Procedures (for Linux and Mac Workstations):

Anti-virus software must be activated.

If something unusual happens, the user should log out and then log back in. If the problem persists, the user should report this to their System Administrator. An example of something unusual happening would be if many windows were opened up on the desktop with the user asking this to happen.