

Policy on Workstation Use

(AAP recommended policy modified by PCC)

Sample Policy And Procedures on Workstation Use

Introduction

Our practice has adopted this policy on workstation use to comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Security Standards. It is our duty to protect the confidentiality, integrity, and accessibility of our patients electronic medical information as required by law. Physicians and staff that use the practices information system must be familiar with the contents of this policy and follow its guidance as appropriate when using computer equipment. As an employee of our practice, you are required to abide by the workstation use policy.

Operating Environment

All computers owned by our practice will be connected to surge protectors purchased by the practice.

or

Our practice has an office wide surge suppressor installed in our circuit breaker system.

Employees will monitor the computer system and report potential threats to the security of the data contained in the system to our Security Official. All employees will take appropriate measures to protect computers and data from disasters based on our policies and procedures.

Our employees should keep computer terminals, hard drives, keyboards, and screens clear of food and drink at all time.

The network and workstations have been configured according to standards provided by our practice. The programs that have been installed are for the sole use of our practice. All accessible data, personal or private, is for the sole use of our practice. This includes data that employees may put on their local hard drives. The computer has been set up for your individual use solely for the business of our practice. Employees are not authorized to change any settings unless instructed by the Security Official. The Security Official monitors which software and hardware is at each workstation.

Do not change anything without approval from the System Administrator.

Employees will not subject the practices system to malicious programs (e.g., viruses, worms, etc.).

Passwords

Employees are expected to maintain the confidentiality of their passwords. We expect authorized users to be responsible for the security of their password.

Employees will log on to the system with their own password. Under no circumstances

will an employee share their password with another employee or unauthorized person in order to allow them access to the system. Our practice monitors system access by authorized users.

Content

Employees will be held responsible for the content of any data entered into the system. This includes any information transmitted within the practice or outside the practice. An employee will not hide his/her identity as the author of any entry or represent that someone else entered the data or sent the message.

Our Security Official will issue access authorization to each employee.

No employee may access any confidential patient or other information that they do not need to know. No employee may disclose confidential patient or other information, unless properly authorized.

Employees may only use the computer system including email and fax capability for business purposes.

Printers

When printing confidential patient information, employees are required to attend to the printer.

Do not leave confidential information unattended on a company printer.

Log-off

Note: Practices will need to determine their log off requirements based upon their individual practice situations.

Screen savers will be programmed for each computer to activate after five minutes of idle screen time and to require a user specific password before allowing access to the computer.

When employees leave their computer terminal for any length of time, they are required to log-off the system. Emergent situations are the exception to this rule. The Security Officer will determine emergent situations.

When employees leave their computer terminal for any length of time, the system will automatically log off after ten minutes of idle screen time.

Backup Procedures

Employees are required to adhere to the backup policies and procedures of our practice with regard to all utilized applications.

Device and Media Controls

Employees will use backup media (e.g., tapes, CDs, disks, etc.) that are provided by our practice.

Employees will assume that all electronic media belonging to the practice contains

confidential information.

Destruction Procedures

Employees are required to adhere to our destruction procedures with regard to devices and media that contain EPHI.

Hard drives will be cleaned of all EPHI prior to its resell, donation, or disposal by use of appropriate cleaning software and by running them under the practice's degausser.

If a hard drive fails and is being replaced by a vendor, the failed hard drive must be run under the practice's degausser before it leaves the practice.

Electronic media (e.g., tapes, CDs, disks, etc.) will be degaussed and then destroyed via shredding or incineration prior to disposal.

Sanctions

Any employee found to have violated this policy would be subject to disciplinary action, up to and including termination of employment.

Optional Sections

Shared Portable Computers (optional)

The laptop computers are the sole property of the practice. The laptops are for offsite work based upon prior approval from your supervisor.

The laptops must be checked out from the Security Official so that they can be kept track of for other employees to use.

The laptops are set up by the Security Official when they are purchased. Data needed should be saved on a floppy disk or CD, not to the laptop hard drive. If the data files you need are too large for floppy disks or CDs, the Security Official will load them on the laptop via the network.

When you return to the office, all data must be removed from the laptops immediately, particularly if the files are too large to put on a floppy disk.

The laptop will then be checked back in by the Security Official

When working offsite, you should find some way to keep the data separate from the laptop. In addition, the laptop should be turned off when you are not actively working on it in order to avoid disclosure of confidential or sensitive data. Data security is a must when you are away from the practice setting.

Employees are accountable for the security of the laptop while in their possession. If the equipment is stolen, employees are to report the theft immediately.

Electronic Mail (optional)

The Email system should only be used for work related purposes. The practice reserves

the right to monitor Email and Internet usage.

Due to system restrictions and space limitations, no pictures, graphics, movies, or any other Email file attachments should be in the system without a viable business reason.

Forgery (or attempted forgery) of electronic mail messages is prohibited.

Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.

Attempts at sending harassing, obscene, or threatening email to another user are prohibited.

Attempts at sending junk mail, for-profit, or chain email is prohibited.

Internet Access (optional)

Our practice authorizes the availability of the Internet/World Wide Web to provide access to Internet resources that will enhance and support business activities. It is expected that employees will use the Internet to improve their job knowledge and to access information on topics which have relevance to the practice.

Employees who do not require access to the Internet as part of their official duties will not be given access.

Employees should be aware that when access is accomplished using Internet addresses and domain names registered to the practice, they may be perceived by others to represent our practice. Users are advised not to use the Internet for any purpose that would reflect negatively on our practice or its employees.

Our computer system is not for personal use; however, when certain criteria are met, users are permitted to engage in the following activities:

During working hours, access job-related information, as needed, to meet the requirements of their jobs.

During working hours, participate in Email discussion groups (list servers), provided these sessions have a direct relationship to the user's job with the practice.

The following uses of the Internet, either during working hours or personal time, using the practice's equipment or facilities, are not allowed:

Access, retrieve, or print text and graphics information that exceeds the bounds of generally accepted standards of good taste and ethics.

Engage in any unlawful activities or any other activities that would in any way bring discredit on our practice.

Engage in personal commercial activities on the Internet, including offering services or merchandise for sale or ordering services or merchandise from on-line vendors.

Engage in any activity that would compromise the security of the practice.

Obtaining personal files via the Internet on individual PC hard drives or on local area network (LAN) file servers.

Game playing of any kind.

Propagating any computer virus.

Maintaining a secret pass code.

Employees will follow existing security policies and procedures in their use of Internet services and will refrain from any practices that might jeopardize the computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet.

Employees using equipment owned by the practice to access the Internet are subject to having activities monitored by the Security Official. Use of this system constitutes consent to security monitoring and employees should remember that most sessions are not private.

Confidential information is not to be transmitted over the Internet without encryption.

Personal Digital Assistant (PDA) (optional)

A PDA is classified as a portable electronic device that interfaces with a divisional workstation.

A PDA is primarily used for personal information management, including remote calendar and task management.

The PDA is not considered a secure computing device. It is recommended that only non-confidential information be stored on the device and the password protection feature enabled.

The Security Official must approve installation of a PDA device and associated software. A valid business must be demonstrated beyond the use of the personal information management (PIM) features (e.g., calendar, phone list, to-do list).

All PDAs connected to the our network, whether supplied by the employee or the practice, shall comply in total with the standards for PDA hardware and software.

PDAs shall include: Hardware, desktop software, synchronization software, backup software.

The practice has the right to require the removal of specific software or files from PDAs connecting to the network, whether employee or practice-owned.

Practice-owned PDAs are assigned to a specific position. When a position for which a PDA was approved is vacated, the practice-owned PDA, software, and accessories will be returned to that position's supervisor.

Employee-owned: Upon leaving the position for which a PDA was approved, all practice-owned software or information will be removed and practice-owned software and accessories will be returned to Security Official.

The practice will provide support for installation of our standard software in connection

with PDAs. Support for PDA hardware is via the hardware vendor.

The practice will perform problem determination activities to establish whether a problem is hardware or software related.

All PDA devices connected to the the practice's network environment, whether employee or practice-owned, shall have password protection enabled.

All PDA devices may be inspected on a yearly basis for existence of unauthorized software or organization data. (Unauthorized Software: For the purposes of this policy, unauthorized software shall include software not licensed for use by the practice, unauthorized duplicate of licensed software, software where proof of ownership cannot be established, or software specifically disallowed by our practice.

Remote Access (optional)

This policy applies to our employees, contractors, vendors, and agents with a practice-owned or personally-owned computer or workstation used to connect to our network.

This policy applies to remote access connections used to do work on behalf of our practice, including reading or sending email and viewing intranet web resources. Remote access means any access to our network through a non-practice controlled network device or medium.

Employees, contractors, vendors, and agents with remote access privileges to our network are required to ensure that their remote access connection is given the same consideration as the user's on-site connection to our network.

Please review the encryption policy for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of our network.

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication.

At no time should any employee provide his/her login or email password to anyone, not even family members, coworkers, or bosses.

Employees with remote access privileges must ensure that their practice owned or personal computer or workstation, which is remotely connected to the practices network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

Employees with remote access privileges to our network must not use personal email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct practice business, thereby ensuring that official business is never confused with personal business.

Reconfiguration of a home users equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

Frame Relay must meet minimum authentication requirements of DLCI standards.

All hosts that are connected to our internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here),

which includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.

Personal equipment that is used to connect to our networks must meet the requirements of equipment owned by the practice for remote access.