



SAMARITAN HEALTH SERVICES
MANUAL OF ADMINISTRATIVE POLICIES

COMPUTER USAGE AND SECURITY

APPROVED: Larry A. Mullins

DATE SIGNED: May 7, 2004

PURPOSE

This policy is to help protect Samaritan Health Services (SHS) and its employees from liability and business interruptions due to inappropriate use of computers and breaches of computer security.

This policy documents the responsibility of computer users to safeguard computer equipment and information from accidental or deliberate unauthorized access, tampering, snooping, distribution, or destruction. It sets forth what is and is not appropriate use of SHS computers. This policy does not purport to address every computer operating and security issue. Information Services (IS) should be contacted if an issue is identified or a situation occurs and a user is uncertain how to deal with it.

This policy is subordinate to any collective bargaining agreement, employment contract, or other employment agreements. SHS may add to or change this policy at any time.

SUMMARY

This policy documents the responsibility of computer users to safeguard computer equipment and information. The summary of this responsibility follows.

- Computer users are responsible for the appropriate use of computers and for taking reasonable precautions to secure the information and equipment entrusted to them.
- Attempting to access SHS computers without specific authorization is prohibited.
- Only Information Services is authorized to install software on SHS computers.
- Using confidential information for other than its intended and approved use is prohibited.
- Important, confidential, or proprietary information should be stored on the local area network rather than on individual computers.
- SHS-licensed software may be reproduced only in accordance with the terms of the software licensing agreements.
- Installing software and making changes to computer hardware, software, and system configuration are prohibited.
- Computer software and equipment purchases must be approved by the IS Steering Committee.
- Incidental and occasional personal use of SHS computers is permitted for reasonable activities.
- Employees are required to report violations or suspected violations of this computer policy.
- Audits to verify that SHS computers are clear of viruses and used in accordance with SHS policy may be performed.
- Audits require authorization of the president/chief executive office of SHS.
- Internet connections are authorized for specific business needs only.
- Incidental or occasional use of e-mail for personal reasons is permitted.

SECURITY POLICY

Responsibility of Computer Users

Computer users are responsible for the appropriate use of SHS computers, and for taking reasonable precautions to secure the information and equipment entrusted to them. Employees are responsible for reporting inappropriate use of SHS computers, breaches of computer security, and assisting in resolving such matters. Users are responsible for adhering to SHS policies and practices as described herein and in other SHS policy manuals to ensure SHS computers are used in accordance with company policy guidelines and reasonable measures are taken to prevent loss or damage of computer information and equipment.

Unauthorized Access

Unauthorized access to SHS computers is prohibited. Attempting to access SHS computers without specific authorization is prohibited. Any form of tampering, including snooping and hacking, to gain access to computers is a violation of SHS policy and carries serious consequences. Employees are required to turn computers off at the end of the day and when not in use for extended periods of time. This will help prevent computer security breaches and damage due to power surges. In addition, computer users must take reasonable precautions to prevent unauthorized access to SHS computers.

Computer Sabotage

Destruction, theft, alteration, or any other form of sabotage of SHS computers, programs, files, or data is prohibited and will be investigated and prosecuted to the full extent of the law.

Password Selection and Protection

Users should select passwords that would be difficult to guess. Passwords should be changed any time there is a concern that they might be compromised. Where possible, passwords will be selected and changed by the users. Users will be held accountable for password protection. Users should not share passwords with anyone. Passwords should not be written down where they could be found by others, and should not be sent over the Internet, Intranet, or e-mail.

A password that is unique to the user should be selected, and should be used at least once each day. The following guidelines should be observed for password selection:

- The password should be six or more alphanumeric characters, including at least one embedded numeric character.
- The password should not include the user's name, log-in name, name of spouse/partner, name of child or pet, or any other names commonly known to others.
- The password should not be a word pertaining to SHS, the user's work, or an activity the user participates in or follows that is commonly known.
- The password should not include anything derogatory, offensive, or defamatory.

Questions regarding password selection or safekeeping should be directed to the user's supervisor or IS.

Access and Password Protection

Computers should not be left unattended following login or for extended periods of time. Users should not log onto the system if someone can see the user keying in his/her password. Computers are to be turned off when the user leaves at the end of his/her shift. If a remote access program is used and it is necessary for the user to leave the computer on, the user should ensure that it is in a locked room.

Snooping

Snooping into SHS information systems is a violation of SHS policy. Watching other users enter information and looking at computer disks belonging to others is prohibited. Obtaining or trying to obtain passwords for other users or using programs that compromise security in any way is a violation of SHS policy. If someone is observed snooping, it should be reported to SHS management.

Hackers

Except when working with the SHS help desk, information about computer systems access should not be given over the telephone. Obtain the name and telephone number of anyone requesting such information, and tell him/her that someone will return the call immediately. The call should then be reported immediately to IS or SHS management.

Trying to access SHS information systems using hacker techniques is prohibited. Trying to hack into third-party computer systems using SHS computers is prohibited and will be reported to local authorities. Hacker crimes result in millions of dollars in downtime, lost data, and other problems. Anyone caught hacking is committing a serious offense.

Viruses, Worms, and Trojan Horses

It is critical that data and software installed on SHS computers are free of viruses. Data and software that have been exposed to any computer, other than SHS computers, must be scanned before installation. This includes downloads from the Internet and other sources of data that may be contaminated. E-mail attachments should not be opened if the sender is unknown. Viruses can result in significant damage and lost productivity. If a user is uncertain whether data or software should be scanned before installation, contact the IS help desk.

Only IS is authorized to install software on SHS computers. Contact SHS IS when there is a need to have software installed. Software not authorized and installed by IS will be removed from computers.

Use of virus, worm, or Trojan horse programs is prohibited. If a virus, worm, or Trojan horse is identified, or if one is suspected, the user should not attempt to fix the problem. The computer should be turned off immediately, notes should be made as to what was observed, and the IS help desk should be contacted.

CONFIDENTIALITY

General

All computer information is considered confidential. Unless permission has been received for its use, no attempt should be made to access it. Accessing or attempting to access confidential data or information is strictly prohibited. Confidential information should only be used for its intended purpose. Using confidential information for anything other than its intended and approved use is prohibited. Refer to the "Confidential and Proprietary Information" Policy for more information (SHS Manual of Administrative Policies).

Handling Confidential Information

The following actions are inappropriate (under normal circumstances) when dealing with confidential information and should be avoided:

- Printing to a printer in an unsecured area where documents may be read by others.
- Leaving a computer unattended with confidential files logged on.
- Leaving computer disks with confidential data unattended in easy to access places.
- Sending confidential information over the Internet, Intranet, dial-up modem lines, or other unsecured communication lines without approval from department management and IS management.

If a user observes a document at a shared printer, or at any other location, it should not be read without permission.

Encryption

Because different encryption programs and utilities offer different levels of security, the use of encryption and encryption utilities is prohibited without the approval of Information Services. If a user needs to send confidential or proprietary information over the Internet or other public communication lines, approval must be obtained from department management and IS.

PHYSICAL SECURITY

Locks

Physical security is a key in protecting computers and computer information from loss and damage. Floppy disks and other sensitive information should be stored in a locked drawer. Computers should be turned off when not in use for extended periods of time. Office doors should be locked when the office is not occupied for extended periods of time.

Laptop Computers

Laptop computers are difficult to secure. The following are required when laptops are taken off SHS property:

- Lost or stolen computers are to be reported immediately.
- All important files must be backed up. All back-up disks must be stored in a separate physical location from the computer.
- Management authorization is required when removing confidential, important, and proprietary data from the facility.
- Patient information should not be stored on laptops without management authorization.
- Reasonable precautions should be taken to safeguard laptops against accidental damage.
- Laptops should always be stored in concealing carrying cases.

Off-site Computers

Off-site computer use requires additional precautions to safeguard information and equipment, including but not limited to:

- Safeguarding the computer and information from theft or damage.
- Prohibiting access to the computer by family, friends, associates, and others for any purpose without management authorization.
- Adhering to all computer policies and practices of SHS for on-site users.

Personal Digital Assistants, Cell Telephones, and Other Hand-held Devices

Use of a hand-held device requires not only the physical security of the device, but the added precaution to avoid writing down passwords, allowing cached passwords (passwords stored on other computers), and leaving confidential files unencrypted. Unauthorized monitoring of wireless transmissions is possible. In addition, it is almost impossible to determine when or if someone is intercepting wireless traffic. Therefore, wireless users are urged to exercise extreme caution with respect to confidential, proprietary, and personal information.

Hand-held devices used for e-mail that are lost or stolen must be reported immediately to the device vendor and the manager of SHS IS to ensure the device service is terminated. In addition, hand-held devices used for e-mail may not be used by anyone other than the authorized user.

ADMINISTRATIVE MATTERS

Back-up

Important, confidential, or proprietary information should be stored on the Local Area Network (LAN) rather than on individual computers. The network is equipped with electronic and physical security. Activity on the network is monitored for tampering and other security breaches. Maintenance and back-up are performed daily on the network. Programs and other information are updated on the network on a regular basis.

Copyright Infringement

SHS does not generally own computer software, but rather licenses the right to use it. Accordingly, SHS-licensed software may only be reproduced by authorized SHS officials in accordance with the terms of the software licensing agreements. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material are strictly prohibited. Copyright laws apply on the Internet as well. Copyright infringement is serious, and SHS strictly prohibits any such activity. When questions about copyright infringement arise, they should be discussed with management immediately.

Copies of shareware or "free" programs or software must be registered with IS. Department supervisors and the manager of IS must approve all requests for these application programs.

Harassment, Threats, and Discrimination

It is SHS policy and the law that employees are able to work free of unlawful harassment, threats, and discrimination. Unlawful harassment is physical or verbal behavior directed towards an individual due to race, age, marital status, gender, disability, religion, or nationality for the purpose of interfering with an individual's work performance, or creating an intimidating or hostile work environment. It is inappropriate to use SHS computers to share personal views about religion, politics, sexuality, or any other subject of a personal nature that could be considered offensive to others within or outside SHS.

Accidents, Mistakes, and Spills

Users should carefully read computer screens before deleting, saving, or transmitting files. In addition, reasonable precautions should be taken with respect to computer operations, maintenance, handling, and transportation. Extreme caution should be taken when placing liquids and other food items on desks near computers.

Unauthorized Changes to Company Computers

Installing software and making changes to computer hardware, software, and system configurations are prohibited. Periodic audits will be performed, and unauthorized software will be deleted, hardware removed, and system settings restored.

Purchases of Computer Software and Equipment

Computer software and equipment purchases are to be approved by either the IS Steering Committee or the PC Advisory Committee. Purchases are prohibited without this approval. All computer software and hardware purchases must be initiated through IS.

Personal Use of Computers

Incidental and occasional personal use of SHS computers is permitted for reasonable activities that do not need substantial computer hard disk space or other computer equipment. Prohibited activities include, but are not limited to, computer games, personal software and hardware, and operating a personal business on the side. Using SHS computers to store or transmit inappropriate jokes, junk mail, chain letters, or to solicit for commercial, religious, charitable, or political causes is prohibited. A user who is uncertain about a specific activity should contact his/her supervisor. Personal files, information, and use of SHS computers will be treated no differently by SHS than business use with regard to employee privacy.

Proprietary Information

SHS data, databases, programs, and other proprietary information represent SHS assets and may only be used for authorized SHS business. Use of SHS assets for personal gain or benefit is prohibited. Unauthorized sharing of SHS proprietary information with SHS personnel or third parties is prohibited.

Reporting Policy Violations

Employees are required to report violations or suspected violations of this computer policy. Activities that should be immediately reported to management include, but are not limited to:

- Attempts to circumvent established computer security systems.
- Use or suspected use of virus, Trojan horse, or hacker programs.
- Obtaining or trying to obtain the password of another user.
- Using the computer to make harassing or defamatory comments, or to create a hostile work environment in any way.
- Using the computer to communicate inappropriate messages or jokes that may be considered offensive by others.
- Illegal activity of any kind.
- Trying to damage the SHS organization or an employee of SHS in any way.

Computer policy violations will be investigated. Noncompliance with SHS policies may result in discipline up to and including termination. Employees who report violations or suspected violations of the SHS policy will be protected from discrimination, harassment, and any other form of retaliation. Hackers, snoopers, password stealers, virus installers, data erasers, and anyone involved in such activity will be disciplined.

An employee identifying any computer security vulnerability is required to report it immediately.

Termination of Employment

All information on user computers is considered SHS property. Deleting, altering, or sharing confidential, proprietary, or any other information upon termination requires management authorization. The computer entrusted to a user must be returned along with the password, identification code, and any other appropriate information necessary for SHS to continue uninterrupted use of the computer and information.

The following activities are prohibited upon termination and will be prosecuted to the fullest extent of the law:

- Accessing SHS computers.
- Providing third parties or anyone else with access to SHS computers.
- Taking computer files, data, programs, or computer equipment.

PRIVACY

Monitoring Computer Communications and Systems

It is management's fiduciary responsibility to monitor computer activity in order to:

- Provide a professional work environment where computer misuse is not tolerated.
- Reduce the risk of liability and business interruption to the organization.
- Establish and enforce policies to help prevent illegal acts and the violation of individual rights.

Audits to verify that SHS computers are clear of viruses and used in accordance with SHS policy will be performed. SHS will investigate complaints about inappropriate images on computers, inappropriate e-mail, or other inappropriate conduct. SHS will monitor Internet activity to see what sites are accessed, duration of time spent, files downloaded, and information exchanged. Audits require authorization of the president/chief executive officer of SHS and will be initiated by the vice president/chief information officer. Computer systems and information are SHS property and should be used principally for business purposes.

Lawsuits and Subpoenas

SHS computers, like any other SHS-owned property, are subject to subpoenas. This means that prosecutors and plaintiff attorneys may access SHS computers and look at information to gather evidence regarding a complaint.

It is not management's intention to suggest that employees remove any information from computers now or at any other time to in any way hinder an investigation of any kind. Quite the contrary, SHS management prohibits such activity. It is management's intention to ensure that users conduct their work to the highest ethical standard with the knowledge that computer information (even deleted files) can be used against employees and SHS in legal proceedings.

EXTERNAL COMMUNICATIONS

Third Parties

The same standards of decorum, respect, and professionalism that guide employees in the office environment apply to computer communications with third parties. Important, confidential, and proprietary information is stored on SHS computer systems. Accordingly, only SHS personnel are allowed access to the SHS information systems without written authorization from management. Management must approve data and other information received by or provided to third parties.

Dangers of the Internet

Copyright laws can be enforced on the Internet. Viruses can be downloaded from the Internet. Inappropriate web sites, images, and communications exist on the Internet. Competitors exist on the Internet. Hackers exist on the Internet. Therefore, users must follow established computer operating policies and practices to reduce the opportunity for security breaches and inappropriate or illegal activity resulting from connecting to the Internet.

Internet Connections

Internet connections are authorized for specific business needs only. Connection to the Internet without authorization from IS is prohibited. In addition, the following activities are prohibited:

- Downloading programs, pictures, screen savers, and attachments.
- Exploring the Internet for fun or profit.

- Establishing communications with third parties (chat rooms).
- Transmitting unencrypted, confidential, patient, medical, or proprietary information.
- Representing SHS without authorization.

Individuals who have received management approval to transmit information on the Internet should understand that such transmissions are identifiable and attributable to SHS. The Internet should be considered a public forum for all transmissions. All communications on the Internet provide an opportunity for a permanent record and could be edited and retransmitted. Accordingly, maintain a professional decorum in all communications and transmissions.

The following actions are prohibited under all circumstances:

- Portraying oneself as someone else.
- Accessing inappropriate web sites, data, pictures, jokes, files, and games.
- Inappropriate chatting, e-mail, monitoring, or viewing.
- Harassing, discriminating, or in any way making defamatory comments.
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes.
- Gambling or any other activity that is illegal, violates SHS policy, or is contrary to the interest of SHS.

Remote Access

Users are required to turn off dial-up modems at the end of the day. Users are required to turn off remote access programs within a reasonable time after use, usually five to ten minutes. Exceptions require department and IS management approval. Downloading or uploading confidential or proprietary information requires approval by department and IS management.

E-MAIL

Electronic Communications

Incidental or occasional use of e-mail for personal reasons is permitted. However, only SHS personnel are allowed access to the SHS e-mail system. The following e-mail activities are prohibited:

- Accessing or trying to access another user's e-mail account.
- Obtaining or distributing another user's e-mail account.
- Using e-mail to harass, discriminate, or make defamatory comments.
- Using e-mail to make off-color jokes or send inappropriate e-mail to third parties.
- Transmitting SHS records within or outside SHS without authorization.
- Transmitting junk mail, chain letters, gambling information, or soliciting for commercial, religious, charitable or political causes.
- Transmitting patient identifiable information.
- Transmitting complaint/incident investigation information.

- Transmitting peer review information.
- Transmitting personnel performance issues.

Employees are required to report inappropriate use of e-mail.

Spam

Sending unsolicited messages or files to individuals, groups, or organizations that you do not have a prior relationship with is prohibited. Sending messages or files with the intent to cause harm or damage to the intended receiver is a violation of SHS policy and will be prosecuted to the full extent of the law.

INTRANET

Data, programs, and other information are updated regularly on the Intranet. As such, it is the responsibility of employees to ascertain that information they are working with is current.

The same standards of decorum, respect, and professionalism that guide employees in the office environment apply to the use of the Intranet. Important, confidential, and proprietary information is stored on the Intranet. Accordingly, only SHS personnel are allowed access to the Intranet without written authorization from management. All SHS Internet policies apply to use of the Intranet. The following activities are prohibited without management authorization:

- Installation of a web site, page, or any other information.
- Installation of business or personal software on the Intranet.
- Exceeding authorized access of Intranet programs, data, and files.
- Assisting anyone outside SHS in obtaining access to the Intranet.
- Making any changes to the Intranet hardware or software.

FACSIMILE (FAX) MACHINES

Medical information may be transmitted via fax only when it is (1) needed for patient care, or (2) required by a third-party payor for ongoing certification of payment for a hospitalized patient. The information transmitted should be limited to that necessary to meet the requestor's needs. The following guidelines apply when faxing information:

1. Obtain a completed and signed authorization prior to the release of patient information for routine disclosure of information to insurance companies, attorneys, or other legitimate users. This includes information relating to treatment for psychiatric conditions or drug/alcohol abuse.
2. Use a cover sheet that contains the total number of pages being sent, names of sender and receiver, telephone number and fax number of receiver, and the following statement:

"This facsimile may contain confidential or privileged information. It is intended only for the use of the person or office to which it is addressed. If you are not the intended recipient, any disclosure or copying of this facsimile, or taking any action based upon it, is strictly prohibited. If you have received this facsimile in error, please notify this office immediately at the telephone number listed to arrange for its return."
3. Use a call-back and verification when transmitting medical information to ensure appropriateness of release, completion of transmission, and confidentiality.
 - a. The sender will contact the requestor prior to transmission to ensure his/her availability and again immediately after transmission to verify receipt.
 - b. The transmittal record provides the fax number dialed. If the fax number is incorrect, immediately fax a cover sheet to the incorrect number asking the recipient to call back immediately. When the call is received, request that the documents be mailed back as soon as possible.
4. Information regarding HIV testing and HIV results has special protection according to state law and should not be transmitted by fax. This includes references to tests being ordered and/or performed. Procedures for routine release of medical information should be used when releasing HIV test information, i.e., obtaining specific written authorization from the patient and sending via mail service. In the event it is necessary to fax

HIV information, the manager or designate of the Medical Records Department should be consulted prior to transmission.

SUBMITTED BY: SHS Information Services
EFFECTIVE: November 2002
REVIEWED:
REVISED: 5/04

**RECEIPT OF
EMPLOYEE COMPUTER OPERATING AND SECURITY POLICY**

I have received and read the SHS Computer User and Security Policy. I understand that I am responsible for adhering to the policies and practices described therein. I understand that these policies may be added to or changed by SHS at any time. It is my responsibility to bring any questions I have about this policy to my supervisor. I further understand that it is my responsibility to report any violations of this policy that I witness or become aware of during the course of my employment.

PRINTED Employee Name

Department

Employee Signature

Date

GLOSSARY OF TERMS

Computer Information. Data, software, files, and any other information stored on company computers and systems.

Encryption. The process of turning plain text into cipher text by applying an algorithm that rearranges or changes its input into something unrecognizable.

Firewall. A specifically-configured system that serves as a secure gateway between an outside network (e.g., the Internet) and the organization's internal networks.

Hacker. Slang for an individual who attempts and/or succeeds in illegally accessing computer hardware and software.

Hot Links. A connection made between application programs so that when changes are made to the data in one file, the changes appear instantly in another.

Intranet. An internal network that may not be connected to the Internet, but which has some similar functions.

Internet. The Internet is a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people world-wide. Physically, the Internet uses a portion of the total resources of the currently-existing public telecommunication networks. Technically, the Internet is distinguished by its use of a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol). Two recent adaptations of Internet technology, the Intranet and the Extranet also make use of the TCP/IP protocol.

ISDN. Integrated Services Digital Network. Digital telecommunications lines that can transmit both voice and digital network services and are much faster than the highest speed modems.

LAN. Local Area Network. A set of connections between computers that provides the basis for electrical transmissions of information, generally within a small geographical location to serve a single organization.

Login. A start-up file stored in the user's directory. This file is used to execute commands that should only be executed at login time, such as establishing the terminal type and starting windows systems.

Modem. Short for modulator-demodulator. A hardware device that allows two computers to communicate over ordinary telephone lines.

PDA. Personal Digital Assistants.

RAM. Random Access Memory. The working memory of the computer. RAM is the memory used for temporarily storing data while working on it, running applications programs, etc. "Random access" refers to the fact that any area of RAM can be accessed directly and immediately.

Server. A computer or device that administers network functions and applications.

Trojan Horse. A program that masquerades as something it is not, usually for the purpose of breaking into an account or executing commands with another user's privileges.

Virus. A set of instructions that can reside in software and can be used to destroy other files or perform other tasks with another user's privileges.

Web Site. A server computer that makes documents available on the World Wide Web. Each web site is identified by a host name.

Worm. A program that propagates by replicating itself on each host in a network with the purpose of breaking into systems.